# Citrix Virtual Aplicativos e Desktops™ 7 2402 LTSR

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

> O Citrix Virtual Apps and Desktops 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 impulsiona a produtividade.

O programa de Versão de Serviço de Longo Prazo (LTSR) para Citrix Virtual Apps and Desktops oferece estabilidade e suporte de longo prazo para as versões do Citrix Virtual Apps and Desktops.

O Cumulative Update 2 (CU2) é a atualização mais recente para o LTSR 2402. Os LTSRs também estão disponíveis para Citrix Virtual Apps and Desktops 1912 e 2203.

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

## Versões anteriores

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

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

# Citrix Virtual Apps and Desktops no Citrix Cloud™

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

## Links úteis

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

# Novidades

## Atualização Cumulativa 4 (CU4)

Data de lançamento: May 08, 2026

### Sobre esta versão

O Citrix Virtual Apps and Desktops 7 2402 LTSR Cumulative Update 4 (CU4) corrige mais de 30 problemas relatados desde o lançamento inicial do 2402 LTSR.

2402 LTSR (informações gerais)

2402 LTSR (recursos e informações de atualização)

Novidades nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2402 LTSR (versão inicial)

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

### Downloads

Citrix Aplicativos e Desktops Virtuais 7 2402 LTSR CU4

### Novas implantações

#### Como faço para implantar o CU4 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU4 - usando o metainstalador do CU4. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Examine a seção Citrix Virtual Apps and Desktops 7 2402 LTSR (versão inicial) e preste muita atenção às seções Visão Geral Técnica, Instalar e Configurar e Segurança antes de começar a

planejar sua implantação. Certifique-se de que sua configuração atenda aos requisitos do sistema para todos os componentes.

## Implantações existentes

### O que devo atualizar?

O CU4 fornece atualizações para 15 componentes de linha de base do 2402 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU4. Por exemplo: Se o Citrix Provisioning fizer parte da sua implantação LTSR, atualize os componentes do Citrix Provisioning para o CU4. Se o Citrix Provisioning não fizer parte da sua implantação, você não precisará instalá-lo ou atualizá-lo.

## Componentes de linha de base do 2402 LTSR CU4

| COMPONENTE DE LINHA DE BASE DO 2402 CU4 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| VDA de sessão única | 2402.0.4100.4597 | VDA de sessão única |
| VDA de várias sessões | 2402.0.4100.4597 | VDA de várias sessões |
| Delivery Controller | 2402.0.4100.4597 | Controlador de Entrega(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html#delivery-controller) |
| Citrix Studio | 7.41.4100.46 | Citrix Studio(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html#citrix-studio) |
| Citrix Director | 7.41.4100.33 | Citrix Director(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/director.html) |
| Gerenciamento de Política de Grupo do Citrix | 7.41.4100.40 | Gerenciamento de Política de Grupo do Citrix(/pt-br/citrix-virtual-apps-desktops/2402- |

| COMPONENTE DE LINHA DE BASE DO 2402 CU4 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| | | ltsr/policies/policies-processes.html) |
| Extensão do Lado do Cliente da Política de Grupo do Citrix | 7.41.4100.40 | |
| Citrix StoreFront | 2402.0.4100.21 | Citrix StoreFront(/pt-br/storefront/2402-ltsr) |
| Servidor de Impressão Universal | 7.41.4100.77 | Servidor de Impressão Universal |
| Gravação de Sessão | 24.2.3100 | Gravação de Sessão |
| Linux VDA | 24.02.1100.21 | Agente de Entrega Virtual Linux |
| Gerenciamento de Perfis | 24.2.4100.23 | Gerenciamento de Perfil |
| Citrix Federated Authentication Service | 10.17.4100.21 | Serviço de Autenticação Federada Citrix (FAS) |
| Redirecionamento de Conteúdo do Navegador | 15.48.4100.78 | Redirecionamento de Conteúdo do Navegador |
| Citrix Probe Agent 2206 | 7.41.4100.20 | Baixar |

## Componentes compatíveis com 2402 LTSR CU4

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

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| App Layering | 2206.0.0 | Citrix App Layering |

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| HDX RealTime Optimization Pack | 2.9.400.2702 | HDX RealTime Optimization Pack |
| License Server | 11.17.2.0_BUILD_55100 | Servidor de Licenças |
| Camada de personalização do usuário | 25.11.2 | Camada de personalização do usuário |
| Reprodutor web de gravação de sessão | 24.2.4100.13 | Reprodutor web de gravação de sessão |
| Otimização do Microsoft Teams | 15.32.1000.9 | Otimização do Microsoft Teams |
| Gerenciamento do Ambiente de Trabalho | 2507.1.110.1 | Gerenciamento do Ambiente de Trabalho |
| XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)* | Somente a Atualização Cumulativa mais recente | Documentação |
| VDA 2411 ou superior instalado no Windows Server 2025 com um Delivery Controller CVAD 2402 CUx | 2411.x.x.x | Documentação |

## Exclusões notáveis do 2402 LTSR CU4

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

| COMPONENTES E RECURSOS EXCLUÍDOS |
|---|
| AppDisks™ |
| AppDNA® |

| COMPONENTES E RECURSOS EXCLUÍDOS |
| --- |
| Pacote de Gerenciamento SCOM da Citrix |
| Framehawk |
| vDisk Pessoal |
| Integração Online do Citrix StoreFront |

| 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 de ciclo de vida de fornecedores terceirizados.

## O que há de novo

As seguintes novas funcionalidades e aprimoramentos estão disponíveis no Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 4 (CU4):

Se você estiver no 2203 LTSR CU7, é recomendável seguir um destes caminhos de atualização:

- Atualize para 2402 LTSR CU3 ou uma atualização cumulativa posterior.
- Atualize para 2507 ou uma versão posterior.
- Em geral, é recomendável atualizar para uma versão futura.

### HDX Direct

Agora você pode aumentar o tempo limite do HDX Direct para hosts de sessão multi-sessão para acomodar logons com duração superior a 60 segundos. Consulte as considerações do HDX Direct para obter detalhes.

### Rastreamento Sempre Ativo (AOT)

O Rastreamento Sempre Ativo (AOT) agora é compatível com o Citrix Virtual Apps and Desktops (CVAD) 2402 LTSR CU4 e atualizações cumulativas subsequentes.

O AOT fornece coleta contínua de logs de componentes Citrix compatíveis, permitindo que administradores e equipes de suporte solucionem problemas sem a necessidade de coleta manual de logs ou reprodução de problemas. Os logs são automaticamente encaminhados para um

Servidor de Logs AOT centralizado, tornando-os prontamente disponíveis para análise através do Citrix Director e outras ferramentas compatíveis.

Com esta versão, os clientes que executam o 2402 LTSR CU4 podem implantar o AOT e começar a coletar telemetria de componentes compatíveis, ajudando a reduzir o tempo de solução de problemas e a melhorar o diagnóstico de problemas. Para pré-requisitos de implantação, topologias de implantação compatíveis, compatibilidade de componentes, instruções de instalação e orientação de configuração, consulte a documentação do Rastreamento Sempre Ativo para a versão mais recente.

> **Observação:**
>
> O processo de implantação e configuração do Rastreamento Sempre Ativo é comum em todas as versões CVAD compatíveis, incluindo clientes que executam VDAs em ambientes Citrix Cloud. Consulte a documentação mais recente do AOT para obter as orientações mais atualizadas e os cenários compatíveis.
>
> Para obter mais informações, consulte a documentação do Rastreamento Sempre Ativo

## Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU3:

### Geral

- Ao usar o redirecionamento do Windows Media em um cenário de salto duplo, o Windows Media Player pode travar ou apresentar alto uso da CPU no primeiro salto.
- O Redirecionamento de Conteúdo do Navegador pode falhar ao usar a extensão de Redirecionamento de Conteúdo do Navegador da Microsoft Edge Web Store.
- O Redirecionamento de Áudio Citrix pode parar de funcionar intermitentemente e exigir a reinicialização do serviço.

### Citrix Director

- Ao reproduzir a Gravação de Sessão do Director, alguns links podem abrir via HTTP em vez de HTTPS.

- Você pode experimentar atualizações incorretas de status do host na seção Infraestrutura do painel do Director quando a contagem de hosts excede 10.
- Depois de aplicar os patches de segurança recentes do sistema operacional Microsoft, você pode não conseguir usar o sombreamento Citrix.

### Política do Citrix

- Quando os Virtual Delivery Agents (VDAs) usam contas de usuário do Microsoft Entra ID, as políticas podem não ser aplicadas, o que pode levar a um comportamento de política inconsistente entre as sessões.
- As políticas de grupo do Citrix podem não ser aplicadas às suas máquinas VDA do Windows 365.

### Citrix Studio

- Ao criar um catálogo PVS, a tarefa pode falhar ao listar vDisks, indicando que a cota de tamanho da mensagem foi excedida.
- Ao importar mapeamentos de usuário ou máquina do Active Directory de um arquivo CSV, a importação pode falhar com um erro de "Nomes de usuário não encontrados".
- Você pode não conseguir fazer login no Web Studio como administrador quando um FQDN contiver caracteres interpretáveis por regex.
- Você pode não conseguir realizar ações no Web Studio, como gerenciar tags, quando seu Desktop Delivery Controller tiver a vinculação SSL configurada para um endereço IP específico e o serviço Citrix Orchestration usar incorretamente o endereço IP do localhost.

### Delivery Controller

- Ao adicionar uma conta existente do Active Directory ao pool de identidades, a conta de computador necessária pode não ser criada, o que pode afetar as conexões WebSocket.
- Quando o Serviço Broker se conecta ao Serviço de Confiança FMA, ele pode usar gradualmente mais memória.
- Ao fazer login, o iniciador do Citrix App-V pode exibir erros, especialmente em sistemas não ingleses.
- Ao atribuir pacotes de aplicativos mais recentes a um grupo de entrega no Web Studio, a descoberta de aplicativos pode falhar, de modo que os aplicativos não aparecem no Web Studio e não podem ser atribuídos a grupos de entrega.
- Em ambientes com várias licenças, os usuários finais podem ver um aviso de expiração de licença durante o início da sessão, e os administradores podem ver um aviso no Citrix Studio

se alguma licença no License Server estiver expirada ou prestes a expirar. Esse problema ocorre mesmo quando uma licença válida e ativa para o produto atual está presente.

- Uma condição de corrida durante as transições de estado de licenciamento pode levar a cálculos incorretos do período do modo de cache de licença. Isso impede o início de sessões.
- Quando uma sincronização de configuração ocorre sem alterações significativas de licenciamento, o Serviço de Alta Disponibilidade pode acionar desnecessariamente solicitações do Serviço de Ativação de Licença (LAS).
- O serviço Broker pode falhar durante a enumeração de aplicativos ou desktops, afetando a disponibilidade do serviço.
- Quando ocorre um conflito de tempo entre o Agente de Atualização VDA (VUA) e o instalador ao excluir XenDesktopVDASetup.exe, o VUA pode retomar uma atualização em um VDA que já concluiu sua atualização.
- Quando um thread de heartbeat do VDA para inesperadamente, o Delivery Controller™ pode perder contato com o VDA, fazendo com que o VDA se torne não registrado. Para restaurar o registro, você deve reiniciar manualmente o VDA ou iniciar uma sessão RDP.
- Você pode experimentar uma TokenNotFoundException que impede o lançamento de um aplicativo quando seu dispositivo inicia o lançamento do aplicativo, mas não suporta o compartilhamento de sessão.

#### Serviço de Criação de Máquina

- Em VMs do Windows 11 criadas com Machine Creation Services (MCS), um serviço de agente em segundo plano pode parar, o que pode afetar a estabilidade do sistema.
- Ao criar um catálogo de máquinas que contém apenas um VDA, o MCS sempre coloca o VDA no primeiro local de armazenamento.
- Ao criar ou atualizar um catálogo para máquinas ingressadas no Active Directory no Web Studio com um domínio de pool de identidades que difere do domínio de administrador, a criação da máquina pode falhar.

### Gráficos

### Metainstalador

### Servidor de Impressão Universal

#### Impressão

- A impressão de arquivos grandes em PDF pode falhar

- Você pode experimentar cores de ícones trocadas em PDFs com impressão Enhanced Metafile (EMF).

## VDA para SO de sessão única

### Sessão/Conexão

- Você pode experimentar a interrupção intermitente do redirecionamento da área de transferência entre sua sessão e o cliente.
- Você pode experimentar problemas intermitentes ao iniciar uma nova sessão, onde as máquinas podem travar na tela de boas-vindas.
- Ao usar IPv6, o Studio pode mostrar um endereço de loopback local em vez do endereço de rede esperado no campo “Conectado via”.
- Após reconectar com vários monitores, as janelas de aplicativos do Windows 11 podem ficar ocultas.
- Após reconectar a uma sessão, seu layout de exibição virtual salvo pode não ser aplicado.
- Você pode ouvir um bipe ao colar um nome de arquivo copiado do seu cliente.
- Ao iniciar um aplicativo do Citrix StoreFront, o lançamento pode falhar e exibir a seguinte mensagem de erro: "Não é possível iniciar o aplicativo: {nome do aplicativo}".
- Quando você desconecta e reconecta à sua sessão Citrix em um VDA multissessão do Windows 11, o fuso horário pode ser redefinido, independentemente das suas configurações de fuso horário.

### Exceções do Sistema

- Você pode ter problemas com a instância do contador de desempenho da sessão ICA, pois ela pode estar ausente após a reconexão.
- Você pode ver janelas maximizadas congelarem ou ficarem pretas ao movê-las entre monitores.
- Você pode descobrir que aplicativos publicados congelam ou não respondem enquanto você trabalha ou passa o mouse.
- Você pode ver uma tela azul após a reinicialização em desktops provisionados pelo Citrix Provisioning devido a um erro de driver USB.
- Você pode ter uma falha na tela de login que pode tornar sua área de trabalho sem resposta.
- Você pode descobrir que o Redirecionamento de Conteúdo do Navegador para aplicativos Chrome publicados não redireciona URLs sem extensão.

- O FIDO2 não funciona para edgewebview2 por padrão.
- Você pode descobrir que a instalação do VDA altera uma configuração do Windows, causando falhas no Outlook.
- Você pode encontrar erros de tela azul, como erros de acesso à memória ou de serviço do sistema.
- A autenticação FIDO2 funciona apenas em sessões de navegador, mas falha em aplicativos do Office 365.
- Você pode ter problemas ao verificar a energia restante do dispositivo dentro da sessão, pois o indicador de status da bateria não está visível.
- Você pode ver os menus suspensos de filtro do Excel desaparecerem ao serem redimensionados no modo contínuo.
- O fuso horário da marca d'água pode não ser sincronizado após definir "Usar hora local do cliente" para "Usar fuso horário do cliente".
- O Internet Explorer publicado pode fechar imediatamente ao ser iniciado.
- Você pode ter quedas de áudio de saída ou bipes devido a problemas de áudio UDP.
- Com um único monitor, você pode ver avisos incorretos de tela cheia do HDX 3D Pro quando o HDX 3D Pro estiver desativado.
- Você pode descobrir que os fones de ouvido USB são identificados incorretamente na sessão e aparecem como Citrix HDX Audio.
- Você pode não conseguir fazer login na máquina, após desinstalar o VDA e reiniciá-la.
- A instalação do Citrix VDA em um sistema operacional Windows não inglês em máquinas não ingressadas no domínio pode fazer com que o instalador use nomes de contas de serviço localizados para os serviços VDA. Como resultado, os serviços CitrixVDACeipService e CitrixTelemetryService podem falhar ao iniciar.

## VDA para SO multissessão

### Área de Transferência

### Sessão/Conexão

- Você pode experimentar uma situação em que o lançamento de uma sessão anônima resulta em sessões inesperadas permanecendo ativas em vez de serem fechadas.
- Você pode encontrar um erro de tela azul com o código PAGE_FAULT_IN_NONPAGED_AREA (0x50) intermitentemente devido a um problema no módulo picadm.sys.

- Você pode ter re-registros intermitentes do Serviço de Área de Trabalho e falhas de reconexão.
- Em dispositivos de quiosque, as sessões podem não permanecer maximizadas entre as sessões de usuário.
- Você pode experimentar um pequeno atraso ao reconectar-se a um aplicativo remoto no Windows Server 2016 ou Windows Server 2022.
- O redirecionamento da área de transferência para de funcionar após o estado ocioso em desktops multiusuário.
- Depois de reconectar com vários monitores, as janelas de aplicativos do Windows 11 podem ficar ocultas.
- Depois de reconectar a uma sessão, seu layout de exibição virtual salvo pode não ser aplicado.
- Em uma configuração de monitor duplo onde um VDA está conectado a dois monitores com resoluções diferentes e as telas estão dispostas verticalmente, o cursor do mouse pode saltar do monitor principal para o monitor secundário ao ser movido de baixo para cima em aplicativos contínuos.
- Se o logon do usuário demorar mais do que o esperado, o HDX Direct pode falhar ao ativar para a sessão no VDA 2402 LTSR e no VDA 2507 LTSR CU2 e posterior.

### Cartões Inteligentes

### Exceções do Sistema

- Você pode experimentar uma situação em que o driver de vídeo trava, o que pode interromper sua sessão de área de trabalho.
- Você pode experimentar perda de áudio se o serviço HDX MediaStream parar intermitentemente.
- Você pode não conseguir fazer login, e os processos podem travar, devido a problemas com o serviço Citrix Audio Redirection.
- Você pode encontrar o Microsoft Search sem resposta devido a problemas no serviço de áudio.
- Você pode experimentar uma situação em que os aplicativos publicados em janela podem não ser redimensionados para tela cheia.
- Você pode encontrar erros de tela azul ocasionalmente devido a um problema no driver do sistema.

- O FIDO2 não funciona para edgewebview2 por padrão.
- Você pode encontrar erros de tela azul, como acesso à memória ou erros de serviço do sistema.
- Você pode descobrir que a instalação do VDA altera uma configuração do Windows, causando travamentos do Outlook.
- A autenticação FIDO2 funciona apenas em sessões de navegador, mas falha em aplicativos do Office 365.
- Você pode ter problemas ao verificar a energia restante do dispositivo dentro da sessão, pois o indicador de status da bateria não está visível.
- O redirecionamento da área de transferência para de funcionar após o estado ocioso em desktops multiusuário.
- Você pode ver os menus suspensos de filtro do Excel desaparecerem ao serem redimensionados no modo contínuo.
- O Internet Explorer publicado pode fechar imediatamente ao ser iniciado.
- Ao usar o VDA 2203 CU5 em hosts baseados em AMD Turin, uma tela azul pode ocorrer em picaser.sys.
- Com o redirecionamento FIDO2 ativado, o Microsoft Edge pode ser encerrado inesperadamente após a instalação de uma atualização recente do Windows 11.

### VDA Linux

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gerenciamento de perfil

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gravação de Sessão

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### StoreFront™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

# Atualização Cumulativa 3 (CU3)

Data de lançamento: August 26, 2025

## Sobre esta versão

O Citrix Virtual Apps and Desktops 7 2402 LTSR Atualização Cumulativa 3 (CU3) corrige mais de 30 problemas relatados desde o lançamento inicial do 2402 LTSR.

2402 LTSR (informações gerais)

2402 LTSR (recursos e informações de atualização)

O que há de novo nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2402 LTSR (versão inicial)

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

## Downloads

Citrix Aplicativos Virtuais e Desktops 7 2402 LTSR CU3

## Novas implantações

### Como faço para implantar o CU3 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU3 - usando o metainstalador do CU3. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Consulte a seção Citrix Virtual Apps and Desktops 7 2402 LTSR (initial release) e preste muita atenção às seções Technical Overview, Install and Configure e Security antes de começar a planejar sua implantação. Certifique-se de que sua configuração atenda aos requisitos do sistema para todos os componentes.

# Implantações existentes

### O que devo atualizar?

O CU3 fornece atualizações para 15 componentes de linha de base do 2402 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU3. Por exemplo: se o Citrix Provisioning fizer parte da sua implantação LTSR, atualize os componentes do Citrix Provisioning para o CU3. Se o Citrix Provisioning não fizer parte da sua implantação, você não precisará instalá-lo ou atualizá-lo.

## Componentes de linha de base do 2402 LTSR CU3

| COMPONENTE DE LINHA DE BASE DO 2402 CU3 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| VDA de sessão única | 2402.0.3100.3651 | VDA de sessão única |
| VDA de várias sessões | 2402.0.3100.3651 | VDA de várias sessões |
| Delivery Controller | 2402.0.3100.3651 | Controlador de Entrega |
| Citrix Studio | 7.41.3100.56 | Citrix Studio |
| Citrix Director | 7.41.3100.32 | Citrix Director |
| Gerenciamento de Política de Grupo do Citrix | 7.41.3100.55 | Gerenciamento de Política de Grupo do Citrix |
| Extensão do Lado do Cliente da Política de Grupo do Citrix | 7.41.3100.55 | |
| Citrix StoreFront | 2402.0.3100.14 | Citrix StoreFront |
| Servidor de Impressão Universal | 7.41.3100.89 | Servidor de Impressão Universal |
| Gravação de Sessão | 24.2.3100 | Gravação de Sessão |
| Linux VDA | 24.02.1100.21 | Agente de Entrega Virtual Linux |
| Gerenciamento de Perfis | 24.2.3100.31 | Gerenciamento de Perfil |

| COMPONENTE DE LINHA DE BASE DO 2402 CU3 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| Citrix Federated Authentication Service | 10.17.3100.24 | Serviço de Autenticação Federada Citrix (FAS) |
| Browser Content Redirection | 15.48.3100.106 | Redirecionamento de Conteúdo do Navegador |
| Citrix Probe Agent 2206 | 7.41.3100.23 | Baixar |

## Componentes compatíveis com 2402 LTSR CU3

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

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| App Layering | 2206.0.0 | Citrix App Layering |
| HDX RealTime Optimization Pack | 2.9.400.2702 | HDX RealTime Optimization Pack |
| License Server | 11.17.2.0_BUILD_53100 | Servidor de Licenças |
| Camada de personalização do usuário | 25.3.3 | Camada de personalização do usuário |
| Player web de gravação de sessão | 24.2.3100.12 | Player web de gravação de sessão |
| Otimização do Microsoft Teams | 15.32.1000.9 | Otimização do Microsoft Teams |
| Gerenciamento do Ambiente de Trabalho | 2402.1.100.1 | Gerenciamento do Ambiente de Trabalho |

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)* | Somente a Atualização Cumulativa mais recente | Documentação |
| VDA 2411 ou superior instalado no Windows Server 2025 com um Delivery Controller CVAD 2402 CUx | 2411.x.x.x | Documentação |

## Exclusões notáveis do 2402 LTSR CU3

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

| COMPONENTES E RECURSOS EXCLUÍDOS |
|---|
| AppDisks™ |
| AppDNA® |
| Pacote de Gerenciamento SCOM da Citrix |
| Framehawk |
| vDisk Pessoal |
| Integração Online do Citrix StoreFront |

| 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.

# O que há de novo

As seguintes novas funcionalidades e aprimoramentos estão disponíveis no Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 3 (CU3):

Se você estiver no 2203 LTSR CU7, é recomendável seguir um destes caminhos de atualização:

- Atualize para 2402 LTSR CU3 ou uma atualização cumulativa posterior.
- Atualize para 2507 ou uma versão posterior.
- Em geral, é recomendável atualizar para uma versão futura.

### Notificação de EOL do sistema de licenciamento baseado em arquivo

O sistema de licenciamento baseado em arquivo, tradicionalmente usado para ativar vários componentes locais, será Fim da Vida Útil (EOL) em April 15, 2026. Serviço de Ativação de Licença (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. O LAS será a única forma de ativar e licenciar componentes locais da Citrix após April 15, 2026. Para permanecer compatível, sua implantação do Citrix Virtual Apps and Desktops deve estar em uma versão compatível com LAS. As versões mínimas de CVAD necessárias que são compatíveis com LAS são:

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

Se tiver dúvidas ou preocupações, entre em contato com o Suporte ao Cliente. A Citrix pode limitar ou suspender sua Manutenção Citrix por não conformidade com esses requisitos, sem responsabilidade, além de quaisquer outros recursos que a Citrix possa ter por lei ou equidade. Esses requisitos não se aplicam onde proibido por lei ou regulamento.

### HDX Seguro™

O Secure HDX agora está geralmente disponível. Esta é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que elementos de rede no caminho do tráfego inspecionem o tráfego HDX. Para obter mais informações, consulte Secure HDX.

### Web Studio

#### Seleção de domínio aprimorada

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

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

#### Suporte para a criação de catálogos unidos ao Azure AD Híbrido do Citrix Provisioning™ em ambientes Azure e VMware usando o Web Studio

Com o Web Studio, agora você pode criar catálogos unidos ao Azure AD Híbrido do Citrix Provisioning em ambientes Azure e VMware. Anteriormente, você só podia usar o PowerShell para criar os catálogos unidos ao Azure AD Híbrido no ambiente local do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Criar catálogos unidos ao Azure AD Híbrido

### Delivery Controller™

#### Compatibilidade da versão do Servidor de Licenciamento com o site do Citrix Virtual Apps and Desktops™

Para a criação e atualizações do site do Citrix Virtual Apps and Desktops, certifique-se de que o Servidor de Licenciamento esteja executando no mínimo a versão 11.17.2 build 53100.

## Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU2:

### Citrix Director

- No Director 2402 LTSR, não é possível configurar um servidor SMTP na GUI se a senha tiver mais de 50 caracteres.
- Na versão 2407 e posteriores do Director, o console não é exibido em francês — mesmo que você defina o idioma do seu navegador para fr-CA ou fr-FR.

- Você pode ver "No records to show" (Nenhum registro para mostrar) em vez de sessões desconectadas ou inativas ao clicar no botão “Show all resources” (Mostrar todos os recursos) na visualização “Select a session” (Selecionar uma sessão) no Citrix Director 2402.
- No Citrix Director, os administradores podem ver um erro intermitente ao acessar os filtros de Máquinas ou Sessões. O problema é causado por uma falha no método `AtomValueUtils.ConvertStringToPrimitive`.

### Citrix Policy

- Ao gerenciar políticas de grupo usando o Console de Gerenciamento de Política de Grupo (GPMC), a configuração "VDA upgrade proxy configuration" pode estar indisponível para edição, mesmo após a instalação do CitrixGroupPolicyManagement_x64.msi da versão 2411 ou anterior.
- Após a hibernação, você pode notar que o VDA não aplica GPOs configuradas pelo domínio, levando a um desalinhamento da política após a reinicialização.
- Você pode ter problemas ao carregar políticas geradas usando provedores PowerShell legados no Web Studio.

### Citrix Studio

- Quando um Delivery Controller™ é desligado em uma configuração redundante, você pode não conseguir fazer login no Web Studio a partir do controlador restante. Esse problema ocorre na versão 2402 LTSR e exibe a mensagem: "Unable to sign in. Please try again later." (Não é possível fazer login. Tente novamente mais tarde.)
- Ao criar um catálogo de máquinas via Web Studio, uma exceção pode ser gerada. O problema não é observado no MMC Studio.
- As credenciais do Active Directory falham no Studio for Web ao realizar ações relacionadas ao AD, como adicionar usuários ou máquinas. As mesmas ações funcionam corretamente no aplicativo Studio completo.

### Delivery Controller

- Monitor Service grooming pode falhar devido a um nome de variável inválido na definição da tarefa. Este problema afeta a tarefa `GroomResourceUtilization` e pode impactar outras tarefas de grooming também.
- O agente de atualização do VDA CU fica sem resposta durante a janela de atualização. Como resultado, nem todos os VDAs mostram "atualização disponível" e alguns falham ao instalar dentro da janela programada.

- Depois de atualizar o DDC para 2402 CU1, as sessões de PC Remoto podem parar de funcionar. Este problema afeta apenas os VDAs de PC Remoto.
- Ao fazer login no Web Studio com Administrador de Grupos de Entrega e Escopo personalizado de Grupos de Entrega, você pode encontrar um erro ao tentar excluir uma Tag de uma máquina de SO de sessão única ou de uma máquina de múltiplas sessões, selecionando Gerenciar Tags.

### Serviço de Criação de Máquina

- O VDA Linux do MCS pode ficar não registrado após um certo período de tempo se falhar ao atualizar a senha da máquina.
- No Google Cloud Platform (GCP), a exportação de imagem falha devido a uma imagem obsoleta para a máquina virtual Daisy no 2402 CU2.
- Você pode encontrar um erro ao tentar criar um novo catálogo do Windows 11 híbrido no Web Studio. O processo falha na fase de criação da conta da máquina com o erro: "Set-AcctADAccountUserCert: Object reference not set to an instance of an object."
- A atualização de um Delivery Controller de 2203 CU5 para 2402 CU1 pode falhar durante a atualização automática do site no Citrix Studio. A atualização do Delivery Controller é concluída, mas a atualização do site não é concluída com êxito.

## Gráficos

- Ao usar uma configuração de monitor duplo e compartilhar uma janela de navegador pop-out, o público pode ver o navegador pai em segundo plano.

## Metainstaller

- A atualização do VDA de 2203 CU3 para CU5 redefine todas as configurações de registro em `HKLM\SYSTEM\CurrentControlSet\Services\picadm`, incluindo a remoção da entrada `DisableFullStreamWrite`. Se você espera que essas configurações persistam, talvez seja necessário reaplicá-las após a atualização.
- Após a atualização para o Citrix Virtual Apps and Desktops (CVAD) 2203 CU5 ou 2402, o acesso à instância WMI `Citrix_Client_Enum` pode falhar com um erro de "Provider Load Failure".

## Servidor de Impressão Universal

### Impressão

- Após a atualização do Universal Print Server (UPS) para 2203 LTSR CU5, você pode experimentar longos atrasos ao selecionar uma impressora. A impressora pode permanecer no estado "Conectando à impressora" e levar mais de um minuto para ficar disponível.

## VDA para SO de sessão única

### Sessão/Conexão

- Ao usar o Windows 11 24H2, a sessão trava e exibe uma tela preta durante o lançamento.
- Um erro de tela azul com o código PAGE_FAULT_IN_NONPAGED_AREA (0x50) pode ocorrer intermitentemente devido a um problema no módulo picadm.sys.
- Se você se conectar a um desktop publicado com arrastar e soltar habilitado, e então desconectar e reconectar ou conectar de um cliente diferente onde arrastar e soltar está desabilitado, o arrastar e soltar permanece habilitado até que você faça logoff e inicie uma nova sessão.
- Você pode experimentar um atraso na tela "Encerrando sessão" ao fazer logoff de uma sessão do Windows 10.
- Ao iniciar um aplicativo publicado, uma caixa preta aparece ao lado do aplicativo e permanece visível até você encerrar a sessão.

### Exceções do Sistema

- Em versões anteriores, seu dispositivo pode exibir um erro de tela azul devido a um novo problema com picadm.sys.
- No VDI 1.0, você pode não conseguir ver o vídeo de entrada, usar a pré-visualização própria ou compartilhar sua tela.
- Ao usar o Citrix Workspace para HTML5, o Wfshell.exe pode travar após copiar e colar grandes quantidades de dados no Excel. Este problema não ocorre quando você usa o aplicativo Citrix Workspace instalado localmente.
- Após a atualização para o VDA 2402, o uso da CPU aumenta durante as sessões de aplicativos publicados em ambientes compartilhados.
- Depois de instalar as atualizações do Windows, o cursor do mouse se move de forma imprevisível e pode saltar aleatoriamente em VDAs de sessão única.

## VDA para SO multissessão

### Área de Transferência

- O Citrix WinFrame Shell (WFshell.exe) pode travar depois de copiar e colar conteúdo no Excel, o que interrompe a sessão e impede que você inicie novos aplicativos ou interaja com aplicativos publicados. Este problema ocorre apenas ao usar o Citrix Workspace para HTML e não afeta o Citrix Workspace App.

### Sessão/Conexão

- Você pode ter uma falha na sessão do VDA seguida por uma reinicialização da máquina.
- Com o VDA 2402 LTSR, você pode ver aleatoriamente erros de "Acesso Negado" depois que sua sessão é desconectada inesperadamente. Quando isso acontece, sua sessão desaparece sem aviso e as tentativas de reconexão falham com o mesmo erro.
- Um VDA pode ficar não registrado e completamente sem resposta. Você não pode se reconectar à máquina virtual afetada até reiniciá-la manualmente.
- Um erro de tela azul com o código PAGE_FAULT_IN_NONPAGED_AREA (0x50) pode ocorrer intermitentemente devido a um problema no módulo picadm.sys.
- Se você se conectar a uma área de trabalho publicada com arrastar e soltar ativado, e depois desconectar e reconectar ou conectar de um cliente diferente onde arrastar e soltar está desativado, o arrastar e soltar permanece ativado até que você faça logoff e inicie uma nova sessão.
- Ao iniciar um aplicativo publicado, uma caixa preta aparece ao lado do aplicativo e permanece visível até você fazer logoff da sessão.
- Ao iniciar sessões do Citrix Workspace™ App para Linux, as sessões parecem abrir, mas fecham imediatamente sem mostrar nenhum erro.

### Cartões Inteligentes

- Após a atualização para o Citrix Virtual Apps and Desktops (CVAD) 2402 CU1, você pode ocasionalmente ver falhas no processo `CertPropSvc`. Isso pode causar problemas com o acesso ao cartão inteligente.

### Exceções do Sistema

- Você pode experimentar falhas aleatórias em versões anteriores de VDAs com o código de parada `SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x7E)`.
- Você pode ver sessões de usuário exibidas como "desconhecidas" e falhar ao reconectar após a atualização para o LVDA 2402CU1.

- Em versões anteriores, você não pode expandir janelas SAP horizontalmente usando o mouse em uma tela de laptop sem um monitor secundário.
- Em versões anteriores do CVAD, seu dispositivo pode exibir um erro de tela azul devido a um novo problema com picadm.sys.
- Ao usar o Citrix Workspace para HTML5, o Wfshell.exe pode travar após copiar e colar grandes quantidades de dados no Excel. Esse problema não ocorre ao usar o aplicativo Citrix Workspace instalado localmente.
- Em um cenário de várias sessões, a funcionalidade de copiar e colar pode parar de funcionar se você copiar mais de aproximadamente 2.493 caracteres.
- O CtxSvcHost.exe pode travar durante operações de área de transferência devido a um problema na DLL da Área de Transferência.
- Quando vários servidores LDAP estão inacessíveis, o registro do VDA com o Delivery Controller pode falhar, e as pesquisas LDAP também podem encontrar problemas.
- O script `Enable-VDASSL.ps1` pode não funcionar como esperado ao habilitar o TLS na imagem mestre do VDA.
- A geolocalização do cliente pode não ser redirecionada para o VDI para TSVDA, potencialmente impactando certas aplicações e funcionalidades de segurança.
- Alguns aplicativos publicados podem usar a hora do sistema VDA em vez da hora local do cliente se você iniciar o aplicativo antes que as políticas do Citrix sejam totalmente aplicadas.
- A tela fica sem resposta se o VDA não for usado por 10 a 15 minutos e, em seguida, é necessário reconectar/redefinir o VDA para corrigir o problema.
- Você pode não conseguir mover e arrastar aplicativos App-V contínuos em versões anteriores.
- O redirecionamento de URL do host para o cliente modifica parâmetros de URL que diferenciam maiúsculas de minúsculas, convertendo letras maiúsculas em minúsculas, o que pode causar falhas ao acessar aplicativos que exigem capitalização de letras específica.
- O Redirecionamento de Conteúdo do Navegador não carregará a página redirecionada real e você verá a página de fundo do BCR ("A página foi redirecionada"). Recarregar a página não resolve o problema.
- Após instalar as atualizações do Windows, o cursor do mouse se move de forma imprevisível e pode saltar aleatoriamente em VDAs de sessão única.

### VDA Linux

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gerenciamento de Perfil

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gravação de Sessão

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### StoreFront™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

# Atualização Cumulativa 2 (CU2)

Data de lançamento: February 06, 2025

> **Observação:**
>
> O problema relatado em CTX692777 é resolvido com a versão mais recente do lançamento do CU2.
>
> Os clientes podem fazer upgrade para esta nova versão. As implantações existentes do CU2 continuarão a funcionar.

## Sobre este lançamento

O Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 2 (CU2) corrige mais de 30 problemas relatados desde o lançamento inicial do 2402 LTSR.

2402 LTSR (informações gerais)

2402 LTSR (recursos e informações de upgrade)

Novidades neste lançamento

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2402 LTSR (lançamento inicial)

Problemas conhecidos neste lançamento

Descontinuação e remoções

Datas de elegibilidade do Citrix Product Subscription Advantage

## Downloads

Citrix Aplicativos Virtuais e Desktops 7 2402 LTSR CU2

## Novas implantações

### Como faço para implantar o CU2 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU2 - usando o metainstalador do CU2. Antes de fazer isso, recomendamos que você se familiarize com o produto:

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

## Implantações existentes

### O que devo atualizar?

O CU2 fornece atualizações para 15 componentes de linha de base do 2402 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU2. Por exemplo: se o Citrix Provisioning fizer parte da sua implantação LTSR, atualize os componentes do Citrix Provisioning para o CU2. Se o Citrix Provisioning não fizer parte da sua implantação, você não precisará instalá-lo ou atualizá-lo.

## Componentes de linha de base do 2402 LTSR CU2

| COMPONENTE DE LINHA DE BASE DO 2402 CU2 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| VDA de sessão única | 2402.0.2150.2566 | VDA de sessão única |
| VDA de múltiplas sessões | 2402.0.2150.2566 | VDA de múltiplas sessões |
| Delivery Controller | 2402.0.2150.2566 | Delivery Controller |

| COMPONENTE DE LINHA DE BASE DO 2402 CU2 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| Citrix Studio | 7.41.2150.32 | Citrix Studio |
| Citrix Director | 7.41.2150.21 | Citrix Director |
| Gerenciamento de Política de Grupo do Citrix | 7.41.2150.32 | Gerenciamento de Política de Grupo do Citrix |
| Extensão do Lado do Cliente da Política de Grupo do Citrix | 7.41.2150.32 | |
| Citrix StoreFront | 2402.0.2100.11 | Citrix StoreFront |
| Servidor de Impressão Universal | 7.41.2100.52 | Universal Print Server |
| Gravação de Sessão | 24.2.2100 | Session Recording |
| Linux VDA | 24.02.1100.21 | Linux Virtual Delivery Agent |
| Gerenciamento de Perfis | 24.2.2100.17 | Profile Management |
| Citrix Federated Authentication Service | 10.17.2150.16 | Citrix Federated Authentication Service (FAS) |
| Redirecionamento de Conteúdo do Navegador | 15.48.2100.49 | Redirecionamento de Conteúdo do Navegador |
| Citrix Probe Agent 2206 | 7.41.2150.16 | Baixar |

## Componentes compatíveis com 2402 LTSR CU2

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

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| App Layering | 2206.0.0 | Citrix App Layering |
| HDX RealTime Optimization Pack | 2.9.400.2702 | HDX RealTime Optimization Pack |
| Servidor de Licenças | 11.17.2.0_Build 51000 | Servidor de Licenças |
| Camada de personalização do usuário | 24.9.0 | Camada de personalização do usuário |
| Reprodutor web de Gravação de Sessão | 24.2.2100.7 | Reprodutor web de gravação de sessão |
| Otimização do Microsoft Teams | 15.32.1000.9 | Otimização do Microsoft Teams |
| Gerenciamento do Ambiente de Trabalho | 2402.1.100.1 | Gerenciamento do Ambiente de Trabalho |
| XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)* | Somente a Atualização Cumulativa Mais Recente | Documentação |
| VDA 2411 ou superior instalado no Windows Server 2025 com um Delivery Controller CVAD 2402 CUx | 2411.x.x.x | Documentação |

## Exclusões notáveis do 2402 LTSR CU2

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

| COMPONENTES E RECURSOS EXCLUÍDOS |
|---|
| AppDisks™ |

| COMPONENTES E RECURSOS EXCLUÍDOS |
| --- |
| AppDNA® |
| Citrix SCOM Management Pack |
| Framehawk |
| Personal vDisk |
| StoreFront Citrix Online Integration |

| 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 de ciclo de vida de fornecedores terceirizados.

## O que há de novo

As seguintes novas funcionalidades e aprimoramentos estão disponíveis no Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 2 (CU2):

### Suporte para criar catálogo Citrix Provisioning™ em ambiente VMware usando o Web Studio

Agora você pode criar um catálogo Citrix Provisioning em um ambiente VMware usando o Web Studio. Anteriormente, os administradores tinham que alternar entre diferentes consoles para provisionamento e gerenciamento de catálogos. Este recurso reduz a necessidade de alternar entre consoles e permite que você manipular o provisionamento e o gerenciamento de energia diretamente no Web Studio. Para obter mais informações, consulte Criar um catálogo Citrix Provisioning em ambiente VMware usando o Studio.

### Alterar o mapeamento de sub-rede para o catálogo de máquinas

Anteriormente, para alterar o mapeamento de sub-rede de um catálogo de máquinas, era necessário excluir o catálogo e criar um novo catálogo com o novo mapeamento de sub-rede. Com este recurso, agora você pode obter a mesma funcionalidade alterando o mapeamento de sub-rede no catálogo. Isso garante que as novas máquinas virtuais criadas sob este catálogo estarão no novo mapeamento de sub-rede. Este aprimoramento reduz a sobrecarga de excluir o

catálogo e todas as atividades associadas a ele. Para obter mais informações, consulte Editar um catálogo.

### Integração Pendo

A partir da versão 2402 LTSR CU2, o Web Studio integra o Pendo, que é habilitado por padrão. O Pendo coleta seus dados de uso de acordo com a Política de Privacidade da Citrix. Se você preferir não compartilhar seus dados de uso, pode desativar o Pendo usando a ferramenta de configuração do Studio. Para obter mais informações, consulte Habilitar ou desabilitar o Pendo.

### Lançamento independente do Director para implantações LTSR

O lançamento independente do Director para implantações LTSR agora oferece uma opção para acessar os recursos mais recentes do Director para solução de problemas e monitoramento aprimorados em ambientes Citrix® para ambientes LTSR compatíveis. Este recurso permite que os clientes usem a versão mais recente do Director em suas implantações 2402 LTSR. Além disso, fornece acesso a recursos lançados após o anúncio do LTSR sem impactar a infraestrutura de entrega de aplicativos.

O instalador autônomo inclui os arquivos .msi mais recentes para o serviço Monitor, o serviço Director e o Monitor Snap-in. Usando esses novos arquivos .msi, você pode atualizar seu 2402 LTSR CU1 com os recursos da versão atual.

> **Observação:**
>
> O SQL Server 2016 é incompatível com a versão atual dos serviços Director ou Monitor.

> Para obter informações sobre os recursos do Director que fazem parte das versões atuais após o lançamento do 2402 LTSR, consulte o seguinte:

- Lançamento do Citrix Virtual Apps and Desktops 2407
- Lançamento do Citrix Virtual Apps and Desktops 2411

Para saber mais sobre recursos específicos do Director com a versão mínima do VDA, consulte Matriz de Versões do Director.

#### Principais considerações

- **Atualizações direcionadas:** Acesse os recursos mais recentes em implantações LTSR atualizando apenas o componente Director.

- **Suporte LTSR:** O componente Director e Monitoring Service recém-atualizado não é coberto pelo suporte LTSR, mas o restante da sua infraestrutura LTSR mantém o suporte existente.
- **Opção de reversão:** Você tem a flexibilidade de reverter para a versão anterior do Director, se necessário.

Para obter mais informações, consulte Lançamento independente do Director para implantações LTSR.

### O gerenciamento de imagens agora está geralmente disponível

A funcionalidade de gerenciamento de imagens está geralmente disponível no Citrix Virtual Apps and Desktops 2402 LTSR CU2 para ambientes de virtualização Azure e VMware. Para obter mais informações, consulte Gerenciamento de Imagens.

### StoreFront™

#### Experiência moderna - Disponibilidade geral

A nova experiência moderna agora está geralmente disponível para lojas locais. Esta UI, que antes estava disponível apenas para lojas na nuvem, garante uma aparência consistente em lojas na nuvem e locais. A nova interface de usuário foi projetada para aprimorar e simplificar a experiência do usuário final para acessar aplicativos e desktops Citrix. Ela reduz a complexidade visual, fornece acesso fácil a recursos essenciais e refina a experiência do aplicativo StoreFront. Ela suporta novos recursos, como o Activity Manager, que facilita o gerenciamento eficaz de seus recursos de aplicativos e desktops virtuais. Para obter mais informações, consulte Novidades no StoreFront 2402 LTSR CU2.

## Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU1:

### Citrix Director

- 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.
- Você pode encontrar um problema quando clicar nos detalhes do UserProfile e tentar selecionar texto faz com que a UserProfileBox desapareça, impedindo a cópia de dados.
- Você pode notar que o Director não exibe mais se a conexão HDX™ foi estabelecida usando Secure ICA.

- Você pode experimentar falhas ocasionais de SSON em um Director com balanceamento de carga após a atualização de 2203 CU4 para 2402.
- Em ambientes Director 2402 multi-site, os usuários podem ser desconectados automaticamente do console após 15 minutos de inatividade na página 'Ir para o Site'.
- Os links para a página da máquina na página Filtros no Director estão quebrados no CU1. Você deve procurar a máquina manualmente.
- No Director CU1, você pode ver linhas incorretas selecionadas após a classificação, e às vezes registros extras são adicionados ao selecionar máquinas ou sessões.
- No Citrix Director 2402 CU1, o Gerenciador de Atividades pode não exibir o nome de usuário e, em vez disso, mostra o nome de exibição do usuário.

### Política Citrix

- Você pode experimentar alta utilização de memória do processo CseEngine.exe, o que pode causar problemas de registro de máquina.
- Você pode não conseguir editar ou criar políticas após a atualização para 2402 a partir de uma versão anterior. O problema não ocorre em um site de instalação limpa.
- Após a atualização dos Delivery Controllers (DDCs) e bancos de dados de 1912 para 2402, as prioridades de política no Citrix Studio mudam, afetando todos os sites.
- Quando você instala o Studio em uma máquina Windows 11 Multi-Sessão e abre o Console de Gerenciamento de Política de Grupo, a seguinte mensagem de erro é exibida ao carregar os módulos de Política de Grupo do Citrix: `ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p`.

### Citrix Studio

- No Web Studio 2402 On-Prem, você não pode usar o botão de atualização ao criar ou atualizar um Catálogo de Máquinas.
- Você pode não conseguir fazer login no WebStudio se o domínio tiver um domínio de nível superior (TLD) de um caractere, causando um erro de "token inválido".
- No CVAD Studio 2402 CU1, você pode ver um erro em vez dos detalhes da sessão após remover a coluna Grupo de Entrega da guia Sessão.
- Quando o Nome e o Nome Publicado de um Aplicativo Broker são alterados, o campo "Entregue Como" pode ficar em branco nos detalhes do aplicativo App-V.
- O Web Studio 2402 CU1 pode não exibir as informações do Delivery Controller™ para a métrica de Registro ao recuperar dados do Virtual Delivery Agent (VDA).

## Delivery Controller

- A reconexão da sessão pode falhar se IDs de dispositivo não exclusivos forem relatados, causando problemas com o comportamento da sessão e o desvio dos limites de aplicativos.
- Você pode experimentar alto uso de CPU em um MonitorDB grande que armazena dados por vários meses. Adicionar um índice pode reduzir o uso da CPU em aproximadamente 10-15%.
- No Citrix Virtual Apps and Desktops 2402 On-Prem, o Serviço Citrix Broker mostra alto uso de memória, possivelmente devido a um vazamento de memória, exigindo reinicializações do Delivery Controller a cada 3-4 horas.
- A atualização de um site com várias instâncias do Delivery Controller (DDC) de 2203 CU6 para 2402 pode falhar com o erro "Não é possível comunicar com o banco de dados. Verifique se o banco de dados está em execução" ao atualizar o primeiro Delivery Controller.

### Serviço de Criação de Máquinas

- Você pode encontrar um problema intermitente com o Machine Creation Services™ (MCS) no Citrix 2402, onde apenas metade das máquinas que você tenta adicionar a um catálogo existente são bem-sucedidas. Embora as máquinas apareçam no Active Directory, apenas as bem-sucedidas são exibidas no Studio, e as máquinas com falha não aparecem no seu hipervisor Nutanix até que sejam importadas manualmente do Active Directory.
- No Google Cloud Platform (GCP), a exportação de imagem falha devido a uma imagem obsoleta para a máquina virtual Daisy em 2402.

## Metainstalador

- Ao atualizar do VDA para 2402, a instalação pode falhar com o erro: "A remoção do produto MSI 'MultimediaVideoTs_x64.msi' falhou com o código 'UnknownProduct' (1605).
- Você pode encontrar o erro "As credenciais inseridas são inválidas" ao ingressar no Call Home durante a instalação do VDA 2402 com o recurso Coletar informações de diagnóstico ativado.
- Você pode ter falhas na atualização do VDA em alguns VDAs, com problemas ocorrendo durante a instalação do aplicativo Workspace, especialmente se o aplicativo Workspace já estiver instalado junto com o VDA.

## Servidor de Impressão Universal

### Impressão

- O Serviço de Gerenciamento de Impressão Citrix pode ser encerrado intermitentemente, fazendo com que as impressoras redirecionadas parem de funcionar.

- As impressoras mapeadas pelo cliente podem desaparecer após a reconexão se o serviço de spooler for reiniciado a qualquer momento antes de reconectar a sessão.

## VDA para SO de sessão única

### Área de Transferência

- A cópia de conteúdo usando a opção Copiar para texto e imagem e a cópia de conteúdo formatado podem falhar.

### Sessão/Conexão

- Você pode encontrar um problema em que o logoff de uma sessão ou o encerramento de uma janela de aplicativo publicado leva de 2 a 3 minutos para ser limpo do VDA após a atualização para 2203 CU4.
- As impressoras mapeadas pelo cliente podem desaparecer após a reconexão se o serviço de spooler for reiniciado a qualquer momento antes de reconectar a sessão.
- Você pode experimentar uma falha do processo "explorer.exe" no Virtual Delivery Agent (VDA) ao usar o atalho "Windows + Print Screen.
- Você pode experimentar cintilação contínua da tela na sessão ICA® quando a política de Marca d'água está ativada.

### Exceções do Sistema

- Após a atualização para o CVAD 2203, você pode experimentar um atraso de aproximadamente 10 segundos ao abrir um desktop.
- Você pode ter falhas intermitentes ao usar arrastar e soltar do endpoint para aplicativos e desktops publicados.
- Você pode ter problemas com o recurso de arrastar e soltar que não funciona de forma consistente no Windows 2019 e mais recente, e no Windows 10 e mais recente, ao usar o Citrix Cloud.
- Você pode ter problemas com a falha de redirecionamento da área de transferência da sessão para imagens grandes e gráficos do Excel no VDA, impedindo que você copie e cole esses itens para o lado do cliente.
- Após iniciar um Desktop Publicado, você pode descobrir que a parte superior esquerda da tela não responde, onde os ícones estão visíveis, mas não são clicáveis, a menos que você selecione outros ícones simultaneamente para ativar a área. Esse problema ocorre quando o recurso Arrastar e Soltar está ativado.

- Você pode notar que o áudio não funciona durante as chamadas, pois o Serviço CtxAudio falha aleatoriamente ao usar aplicativos de áudio como o MS Teams.
- Você pode ter falhas aleatórias de redirecionamento USB para usuários clientes, fazendo com que dispositivos USB como Pinpad, TCR e impressoras desapareçam durante a sessão.
- Você pode ter um problema em que os níveis do alto-falante e do microfone de um headset USB são definidos como 0 (mudo) durante a conexão ou reconexão a uma sessão VDI. Esse problema ocorre intermitentemente, e você pode ajustar os níveis manualmente.
- Com o VDA 2402 LTSR, o arrasto de janelas pode não funcionar em aplicativos publicados.

## VDA para SO multissessão

### Área de Transferência

- A cópia de conteúdo usando a opção Copiar para texto e imagem e a cópia de conteúdo formatado podem falhar.

### Sessão/Conexão

- Após a atualização para o VDA 2402, a primeira sessão ICA após uma reinicialização pode exibir uma tela cinza, o que é resolvido desconectando e reconectando ou iniciando uma sessão de aplicativo primeiro.
- Você pode ter um problema em que o logoff de uma sessão ou o encerramento de uma janela de aplicativo publicado leva de 2 a 3 minutos para ser limpo do VDA após a atualização para 2203 CU4.
- Você pode notar um número crescente de itens do Citrix WinFrame Shell na lista de outros ícones da bandeja do sistema, embora apenas um ícone de bateria seja exibido na sessão ICA. Esse acúmulo ocorre nas configurações do sistema em Personalização > Barra de Tarefas > Outros Ícones da Bandeja do Sistema.
- As impressoras mapeadas pelo cliente podem desaparecer após a reconexão se o serviço de spooler tiver sido reiniciado a qualquer momento antes de reconectar a sessão.
- Você pode ter um problema em que os VDAs se tornam aleatoriamente sem resposta e entram em um estado não registrado, fazendo com que os usuários sejam desconectados de suas sessões ICA.
- No Citrix, a geolocalização do cliente não está sendo redirecionada para o VDI para TSVDA quando a sessão ICA se conecta, o que é crítico para certas aplicações e funcionalidades de segurança. Pode ser necessário clicar manualmente em `Refresh` em `GeoLocSync.exe` para que uma sessão ICA substitua.

- Você pode experimentar cintilação contínua da tela na sessão ICA quando a política de marca d'água está ativada.

### Exceções do Sistema

- Você pode ter um problema em que o status da bateria não é exibido no VDA multissessão do Windows 11, apesar de o VDA estar recebendo o status da bateria.
- Você pode experimentar falhas intermitentes ao usar arrastar e soltar do endpoint para aplicativos e desktops publicados.
- Você pode experimentar o recurso de arrastar e soltar não funcionando consistentemente no Windows 2019 e mais recentes, e no Windows 10 e mais recentes ao usar o Citrix Cloud.
- Você pode notar que o evento "MetaFrame 9006" é registrado cada vez que você se reconecta quando o Auto Client Reconnect (ACR) está desativado, criando muitas mensagens de erro indesejadas.
- Você pode ter problemas com a falha de redirecionamento da área de transferência da sessão para imagens grandes e gráficos do Excel no VDA, impedindo que você copie e cole esses itens para o lado do cliente.
- Após iniciar um Desktop Publicado, você pode descobrir que a parte superior esquerda da tela não responde, onde os ícones estão visíveis, mas não clicáveis, a menos que você selecione outros ícones simultaneamente para ativar a área. Este problema ocorre quando o recurso Arrastar e Soltar está ativado.
- Você pode experimentar uma falha no aplicativo de áudio durante o roaming, causada por um travamento no módulo icaendpoint.dll.
- Você pode ter um problema em que o ícone da bandeja do sistema para o aplicativo New Teams publicado não responde a cliques com o botão esquerdo quando está sendo executado como um aplicativo contínuo no SO Windows 2022 com VDA 2402 ou VDA 2402 CU1. Isso só acontece quando o aplicativo está minimizado; funciona bem quando você está em uma sessão de desktop completa.
- Você pode experimentar falhas aleatórias de redirecionamento USB para usuários clientes, fazendo com que dispositivos USB como Pinpad, TCR e impressoras desapareçam durante a sessão.
- O LastPingTime não é atualizado no registro com o 2203 CU5, o que pode fazer com que você seja desconectado.
- Com o VDA 2402 LTSR, o arrasto de janelas pode não funcionar em aplicativos publicados.
- Um bugcheck 0x50 pode ocorrer em wdica32.exe ao ler o estado da licença.

### Serviço de Autenticação Federada

- Você pode enfrentar problemas de desempenho ao gerar certificados de usuário no servidor FAS.

  Para habilitar a melhoria de desempenho, configure a seguinte chave de registro no servidor FAS:

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService

  Nome: SignerCaching

  Tipo: REG_SZ

  Valor: on

### VDA Linux

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gerenciamento de Perfis

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gravação de Sessão

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### StoreFront™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

# Atualização Cumulativa 1 (CU1)

Data de lançamento: August 20, 2024

## Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 1 (CU1) corrige mais de 30 problemas relatados desde o lançamento inicial do 2402 LTSR.

2402 LTSR (informações gerais)

2402 LTSR (recursos e informações de atualização)

O que há de novo nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2402 LTSR (versão inicial)

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

## Downloads

Citrix Aplicativos Virtuais e Desktops 7 2402 LTSR CU1

## Novas implantações

### Como faço para implantar o CU1 do zero?

Você pode configurar um novo ambiente Citrix Virtual Apps and Desktops baseado no CU1 - usando o metainstalador do CU1. Antes de fazer isso, recomendamos que você se familiarize com o produto:

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

## Implantações existentes

### O que devo atualizar?

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

# Componentes de linha de base do 2402 LTSR CU1

| COMPONENTE DE LINHA DE BASE DO 2402 CU1 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| VDA de sessão única | 2402.0.1100.1256 | VDA de sessão única |
| VDA de várias sessões | 2402.0.1100.1256 | VDA de várias sessões |
| Delivery Controller | 2402.0.1100.1256 | Delivery Controller(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html#delivery-controller) |
| Citrix Studio | 7.41.1100.48 | Citrix Studio(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html#citrix-studio) |
| Citrix Director | 7.41.1100.33 | Citrix Director(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/director.html) |
| Citrix Group Policy Management | 7.41.1100.34 | Citrix Group Policy Management(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/policies/policies-processes.html) |
| Citrix Group Policy Client-Side Extension | 7.41.1100.34 | |
| Citrix StoreFront | 2402.0.1100.8 | Citrix StoreFront(/pt-br/storefront/2402-ltsr) |
| Servidor de Impressão Universal | 7.41.1100.58 | Servidor de Impressão Universal |
| Gravação de Sessão | 24.2.1100 | Gravação de Sessão |

| COMPONENTE DE LINHA DE BASE DO 2402 CU1 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| Linux VDA | 24.02.1100.21 | Agente de Entrega Virtual Linux |
| Gerenciamento de Perfis | 24.2.1100.23 | Gerenciamento de Perfil |
| Citrix Serviço de Autenticação Federada | 10.17.1100.16 | Serviço de Autenticação Federada Citrix (FAS) |
| Redirecionamento de Conteúdo do Navegador | 15.48.1100.65 | Redirecionamento de Conteúdo do Navegador |
| Citrix Agente de Sondagem 2206 | 7.41.1100.15 | Baixar |

## Componentes compatíveis com 2402 LTSR CU1

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

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| App Layering | 2206.0.0 | Citrix App Layering |
| HDX RealTime Optimization Pack | 2.9.400.2702 | HDX RealTime Optimization Pack |
| Servidor de Licenças | 11.17.2.0_BUILD_48000 | Servidor de Licenças |
| Camada de personalização do usuário | 24.3.2 | Camada de personalização do usuário |
| Reprodutor web de Gravação de Sessão | 24.2.1100.16 | Reprodutor web de gravação de sessão |

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| Otimização do Microsoft Teams | 15.32.1000.9 | Otimização do Microsoft Teams |
| Gerenciamento do Ambiente de Trabalho | 2402.1.100.1 | Gerenciamento do Ambiente de Trabalho |
| XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)* | Somente a Atualização Cumulativa mais recente | Documentação |
| VDA 2411 ou superior instalado no Windows Server 2025 com um Delivery Controller CVAD 2402 CUx | 2411.x.x.x | Documentação |

## Exclusões notáveis do 2402 LTSR CU1

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

| COMPONENTES E RECURSOS EXCLUÍDOS |
|---|
| AppDisks™ |
| AppDNA® |
| Pacote de Gerenciamento Citrix SCOM |
| Framehawk |
| Personal vDisk |
| StoreFront Citrix Online Integration |

| PLATAFORMAS WINDOWS EXCLUÍDAS * |
| --- |
| Windows 2008 de 32 bits (para Universal Print Server) |

* A Citrix reserva-se o direito de atualizar o suporte da plataforma com base nos marcos de ciclo de vida de fornecedores terceiros.

## O que há de novo

As seguintes novas funcionalidades e melhorias estão disponíveis no Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 1 (CU1):

### Suporte à autenticação por cartão inteligente

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

### Melhoria nos relatórios de telemetria de uso

Com a melhoria no recurso de telemetria de uso de licenças, os dados de utilização de licenças para produtos, componentes e recursos Citrix implantados em ambientes gerenciados pela Citrix são coletados e processados. Esta implementação visa confirmar a conformidade da licença e os dados são gerenciados através do Citrix License Server. Você deve atualizar para a versão mais recente do servidor de licenças e ter uma conta Citrix Cloud™. Para obter mais informações, consulte:

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

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

## Problemas corrigidos

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

### Citrix Director

- Na página Filtros - Todas as Máquinas, ao selecionar todas as máquinas listadas na tela e tentar rolar a lista para baixo, a seleção de objetos não funciona corretamente após uma atualização.
- O layout da tabela aparece limitado a uma pequena parte da tela.
- Na página Máquina de Filtro do Director, depois de escolher a guia "Multi-sessão" e navegar para outra página, ele seleciona a guia padrão Máquinas de Desktop de Sessão Única ao retornar à página Máquina.
- Você pode encontrar um problema ao clicar nos detalhes do UserProfile e tentar selecionar texto, o que faz com que o UserProfileBox desapareça, impedindo a cópia de dados
- Você pode notar que a opção UI.TaskManager.EnableApplications é ignorada na UI, fazendo com que a lista de aplicativos ainda apareça no Director.
- Você pode experimentar falhas ocasionais de SSON em um Director com balanceamento de carga após a atualização de 2203 CU4 para 2402.
- Você pode notar que o Director não exibe mais se a conexão HDX™ foi estabelecida usando Secure ICA.

### Política Citrix

- Você pode portar o GpoScanner para 2404 sem alterar o GpfxSettings.dll
- Você pode experimentar alta utilização de memória do processo CseEngine.exe, o que pode causar problemas de registro de máquina.
- Você pode não conseguir editar ou criar uma política após a atualização para 2402 a partir de uma versão anterior. O problema não ocorre em um site de instalação limpa.
- Você pode encontrar problemas em que a redireção de conteúdo bidirecional falha após a atualização para o Citrix Virtual Apps and Desktops 2402 LTSR

### Citrix Studio

- A console do Studio pode congelar ao usar o Studio como um aplicativo publicado ou ao usá-lo em um VDA publicado sob a sessão ICA®.

### Delivery Controller™

- O serviço 'Citrix.Analytics' falha ao desinstalar o Desktop Delivery Controller (DDC) versão LTSR 2203 CU5 ou ao parar os serviços 'Citrix.Analytics'.

### Machine Creation Service

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

## Gráficos

- Você pode encontrar blecautes intermitentes na tela com duração de aproximadamente 10 segundos durante o trabalho, período em que o processo gráfico do software Citrix (Ctxgfx.exe) é redefinido. O thread twencode experimenta uma exceção de violação de acesso, o que faz com que o ctxExceptionHandler registre minidumps e cause esse problema. O ctxExceptionHandler está configurado para gerar dumps completos para exame.
- Ao iniciar o Desktop, você pode encontrar uma tela preta devido à falha do ctxgfx.

## Metainstaller

- Ao instalar 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.
- Ao tentar instalar o Citrix Virtual Apps and Desktops 2402 pela linha de comando, o comando `Exclude "Local Host Cache Storage (LocalDB)"` não está funcionando como esperado.
- A partir do Citrix Virtual Apps and Desktops 2402, ao usar o comando `/exclude "Local Host Cache Storage (LocalDB)"` no delivery controller, a instalação do software de banco de dados SQL Server Express LocalDB para em vez de continuar a instalação sem o LocalDB.

## Universal Print Server

### Impressão

- Você pode ter serviços de spooler de impressão do Windows travando em VDAs com cpmon.dll, resultando em impressoras perdidas e incapacidade de imprimir após o envio de trabalhos de impressão.

## VDA para SO de sessão única

### Área de Transferência

- Ao usar o VDA 2203 LTSR CU4 e ao copiar e colar conteúdo no formato WebP, `WfShell` para de funcionar.

### Sessão/Conexão

- O aplicativo OpenTEXT ETX não abre devido a uma violação de acesso com o seguinte módulo: C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll
- Você pode ter desligamentos aleatórios de máquinas de sessão única ao fazer a transição para ou sair de períodos de interrupção quando não há sessão ativa.

### Cartões Inteligentes

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

## VDA para SO multissessão

### Área de Transferência

- Ao usar o VDA 2203 LTSR Cu4 e ao copiar e colar conteúdo no formato WebP, `WfShell` para de funcionar.

### Sessão/Conexão

- O aplicativo OpenTEXT ETX não abre devido a uma violação de acesso com o seguinte módulo: C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll
- Você pode ter falhas do TermService com o Citrix VDA.
- Os VDAs podem se tornar não responsivos intermitentemente.
- Você pode encontrar um erro em que os dados do broker da nuvem estão fora de sincronia com o VDA, fazendo com que uma sessão ativa no VDA apareça como desconectada no Director.

### Cartões Inteligentes

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

## Linux VDA

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

## Gerenciamento de Perfis

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gravação de Sessão

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### StoreFront™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

# 2402 LTSR (versão inicial)

## Sobre a versão

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

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

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

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

  Após atualizar seus VDAs para esta versão, você não precisa atualizar o nível funcional do catálogo de máquinas. Para obter mais informações, consulte Versões de VDA e níveis funcionais.

Para instruções de instalação e atualização:

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

# Componentes de linha de base da versão inicial 2402 LTSR

| COMPONENTE DE LINHA DE BASE 2402 | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| VDA de sessão única | 2402.0.4000.4310 | VDA de sessão única |
| VDA multissessão | 2402.0.4000.4310 | VDA multissessão |
| Delivery Controller | 7.41.100.229 | Delivery Controller |
| Citrix Studio | 7.41.100.251 | Citrix Studio |
| Citrix Director | 7.33.4000.26 | Citrix Director |
| Gerenciamento de Política de Grupo do Citrix | 7.41.100.115 | Gerenciamento de Política de Grupo Citrix |
| Extensão do Lado do Cliente da Política de Grupo Citrix | 7.41.100.115 | |
| Citrix StoreFront | 2402.0.100.64 | Citrix StoreFront |
| Citrix Provisioning | 7.41.100 | Citrix Provisioning |
| Servidor de Impressão Universal | 7.33.4000.11 | Servidor de Impressão Universal |
| Gravação de Sessão | 24.2.100.35 | Gravação de Sessão |
| VDA Linux | 24.02.0.93 | Agente de Entrega Virtual Linux |
| Gerenciamento de Perfis | 24.2.100.52 | Gerenciamento de Perfil |
| Serviço de Autenticação Federada Citrix | 10.17.100.90 | Serviço de Autenticação Federada Citrix (FAS) |
| Redirecionamento de Conteúdo do Navegador | 15.32.4000.12 | Redirecionamento de Conteúdo do Navegador |
| Agente de Sondagem Citrix 2402 | 7.41.100.78 | Baixar |

## Componentes compatíveis com a versão inicial do 2402 LTSR

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

| COMPONENTES E RECURSOS COMPATÍVEIS | VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS | DOCUMENTAÇÃO |
|---|---|---|
| HDX RealTime Optimization Pack | 2.9.600 | HDX RealTime Optimization Pack |
| Servidor de Licenças | 11.17.2.0_BUILD_47000 | Servidor de Licenças |
| Camada de personalização do usuário | 23.9.1 | Camada de personalização do usuário |
| Reprodutor web de gravação de sessão | 22.3.4000.4 | Reprodutor web de gravação de sessão |
| Otimização do Microsoft Teams | 15.32.3000.9 | Otimização do Microsoft Teams |
| Gerenciamento de Ambiente de Workspace | 2402.1.100.1 | Gerenciamento de Ambiente de Workspace |

## Exclusões notáveis da versão inicial do 2402 LTSR

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

| COMPONENTES E RECURSOS EXCLUÍDOS |
|---|
| AppDisks™ |
| AppDNA® |
| Pacote de Gerenciamento Citrix SCOM |

| COMPONENTES E RECURSOS EXCLUÍDOS |
| --- |
| Framehawk |
| vDisk Pessoal |
| Integração Online do Citrix StoreFront |

| 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 de ciclo de vida de fornecedores terceiros.

## O que há de novo

Este artigo lista os recursos novos e aprimorados do Citrix Virtual Apps and Desktops™ 7 2402 LTSR. As atualizações são organizadas por componente.

### HDX

#### Secure HDX (Pré-visualização)

Agora você pode usar o Secure HDX, que é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que quaisquer elementos de rede no caminho do tráfego inspecionem o tráfego HDX. Para obter mais informações, consulte Secure HDX.

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

Com a nova política de bloqueio de tela **Permitir Windows** em Gráficos HDX, agora você tem a opção de modificar os tempos limite de exibição do Windows em uma sessão de Área de Trabalho Virtual Citrix no SO Workstation, conforme sua necessidade. Para obter mais informações, consulte Permitir bloqueio de tela do Windows.

#### Novo modo tolerante a perdas para política de áudio

O modo tolerante a perdas para 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 tolerante a perdas para áudio.

### Binários de terceiros assinados

Os binários distribuídos pela Citrix agora são assinados. Binários assinados indicam que são validados por certificados gerados pela Citrix ou por certificados autênticos de terceiros. Para obter mais informações, consulte Instalar VDAs.

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

Com os aprimoramentos nos logs do sistema, o redirecionamento de 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 de conteúdo bidirecional envolvia o gerenciamento de três políticas distintas: Permitir redirecionamento de conteúdo bidirecional, Permitir redirecionamento de URLs para VDA e Permitir redirecionamento de URLs para o Cliente. Essas políticas exigiam configurações tanto no lado do servidor quanto no lado do cliente (configuradas por meio de Políticas de Grupo). A partir desta versão, consolidamos todas as três políticas em uma única política unificada. Isso não apenas simplifica e aprimora o processo de configuração, mas também elimina a necessidade de configurações do lado do cliente. Para obter mais informações, consulte Configuração de redirecionamento de conteúdo bidirecional.

### Redutor HDX

Você pode agora configurar a versão do algoritmo de compressão HDX, ou Reducer, que você deseja usar no host da sessão. Para mais informações, consulte HDX Reducer.

### 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 mais informações, consulte Configurar 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 de registro `msedgewebview2.exe`, pois ela agora está na lista de permissões por padrão.

Para obter mais informações, consulte a documentação Microsoft.

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

Agora você pode usar variáveis de ambiente do sistema no caminho de processos confiáveis. Para mais informações, consulte Usando variáveis de ambiente do sistema.

## Suporte para SCVMM 2025

O Citrix Virtual Apps and Desktops agora oferece suporte ao System Center Virtual Machine Manager (SCVMM) 2025 da Microsoft. Para mais informações sobre os novos recursos suportados no SCVMM 2025, consulte Novidades no System Center Virtual Machine Manager.

## Citrix Secure Private Access™ para local

### Secure Private Access para local e suporte para ZTNA e outras melhorias

A solução Citrix Secure Private Access local 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 web internos e SaaS) usando o portal StoreFront™ local como um portal de acesso unificado a aplicativos web e SaaS, juntamente com aplicativos e desktops virtuais como parte integrada do Citrix Workspace. O Citrix Secure Private Access local é uma solução de Zero Trust Network Access (ZTNA) gerenciada pelo cliente que fornece acesso sem VPN a aplicativos web internos e SaaS com o seguinte, juntamente com uma experiência de usuário final perfeita:

- Princípio do menor privilégio
- Logon 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 para implantações locais – Disponibilidade Geral.

## Virtual Delivery Agents (VDAs) 2402 LTSR

### Opção para instalar, atualizar ou desinstalar o Citrix Workspace App durante a instalação, atualização ou desinstalação do VDA

Este recurso permite que você escolha instalar, atualizar ou desinstalar o Citrix Workspace App durante uma instalação, atualização ou desinstalação do VDA nos seguintes cenários:

- Durante uma instalação do VDA, você pode optar por instalar o Citrix Workspace App. Por padrão, o Citrix Workspace App não é instalado durante a instalação do VDA.
- Durante uma atualização do VDA, se o Citrix Workspace App ainda não estiver instalado no VDA, você pode optar por instalar o Citrix Workspace App.

- Durante uma atualização do VDA, se a versão do Citrix Workspace App puder ser atualizada, a opção de atualizar o Citrix Workspace App será exibida.
- Durante uma desinstalação do VDA, você pode optar por não desinstalar o Citrix Workspace App. Por padrão, o Citrix Workspace App é desinstalado durante a desinstalação do VDA. Para obter mais informações, consulte Selecionar os componentes a serem instalados e o local de instalação e Opções de linha de comando para instalar um VDA

#### Suporte a WebSocket para VDAs

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

Para obter mais informações, consulte Comunicação WebSocket entre VDA e Delivery Controller.

#### Suporte a atualizações de VDA a partir de um compartilhamento de arquivos local ao qual os VDAs têm acesso (Preview)

Agora você pode oferecer suporte a atualizações de VDA a partir de um compartilhamento de arquivos local e especificar o local do instalador do VDA por meio de comandos do PowerShell. Para obter mais informações, consulte Suporte a atualizações de VDA a partir de compartilhamento de arquivos local.

### Web Studio

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

Ao provisionar VMs VMware usando o Machine Creation Service (MCS), agora você pode selecionar um modelo existente como perfil de máquina, permitindo que as VMs dentro do catálogo herdem as configurações do modelo selecionado.

As configurações herdadas incluem:

- Tags colocadas no modelo
- Atributos personalizados
- Políticas de armazenamento vSAN
- Versão do hardware virtual
- vTPM (TPM Virtual) do vSphere
- Contagem de CPU e núcleos por soquete
- Contagem de NIC

Para obter mais informações, consulte Criação de catálogos de máquinas.

### Gerenciando imagens preparadas com o nó Imagens

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

As imagens preparadas usando este nó só podem ser usadas em ambientes Azure e VMware. Para obter informações detalhadas sobre o gerenciamento de imagens, consulte Gerenciamento de imagens (Visualização).

Alternativamente, você também pode criar catálogos com imagens preparadas usando o nó **Catálogos de Máquinas**. Para obter mais informações, consulte Criando catálogos de máquinas.

### Relacionado a políticas

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

### Recursos obsoletos

Os seguintes recursos e configurações foram preteridos no Web Studio:

- Ambientes Azure:

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

- Ambientes AWS:

  A opção **Aplicar propriedades de modelo de máquina a máquinas virtuais**, na página **Configuração do Catálogo de Máquinas > Modelo de Máquina**, foi preterida. Recomendamos usar perfis de máquina para especificar as propriedades da máquina para VMs.

- Todos os ambientes de hipervisor e serviço de nuvem:

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

## Citrix Director

### Integração do Secure Private Access com o Director (Pré-visualização)

A integração do Secure Private Access com o Director permite que o administrador de help desk ou o administrador completo monitore e solucione problemas de todas as sessões do Secure Private Access no Director. Para oferecer suporte a esse recurso, você deve usar as versões 2402 ou posteriores do Director, Secure Private Access, Citrix Workspace app e VDA.

As ações disponíveis incluem a visualização dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário em **Selecionar uma Sessão** pop-up > guia **Sessões** > **Aplicativos Web e Aplicativos SaaS**
- Enumerações falhas ou bloqueadas do Secure Private Access e inicializações de aplicativos falhas na janela pop-up **Selecionar uma Sessão** > guia **Acesso Negado**
- Visualização de detalhes da sessão e do aplicativo para inicializações de aplicativos ativas e falhas
- Visualização de detalhes da sessão e do aplicativo para enumerações falhas e bloqueadas

Para obter mais informações, consulte a página integração do Secure Private Access com o Director (Preview).

### Painel de Métricas de Desempenho Aprimorado

O painel **Métricas de Desempenho** possui uma visualização aprimorada das métricas em tempo real. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados em tempo real, você pode visualizar os dados dos últimos 15 minutos sem esperar pelo tempo de carregamento da página. Esse aprimoramento ajuda a reduzir o tempo médio de resolução, permitindo que os administradores correlacionem várias métricas de desempenho de componentes em uma única visualização. Para obter mais informações, consulte 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 (Preview)

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 MCS (Imagem Preparada) a partir de uma única imagem de origem e usá-la em vários catálogos de máquinas MCS diferentes. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem.

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

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

Para obter informações detalhadas sobre o gerenciamento de imagens, consulte Gerenciamento de imagens (Visualização).

### Verificar várias NICs no VMware

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

### Suporte para a criação de VMs do Windows 11 no GCP

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

Este recurso é aplicável a:

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

Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte Criar VMs do Windows 11 no nó de locatário único.

#### Suporte para a criação de catálogos do Citrix Provisioning™ usando comandos MCS PowerShell no VMware

Agora você pode criar catálogos do Citrix Provisioning usando comandos MCS PowerShell no VMware.

Esta implementação oferece as seguintes vantagens:

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

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

### Gerenciamento de Perfis

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

### VDA Linux

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

### Gravação de Sessão

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

### Workspace Environment Management™

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

### Citrix Provisioning

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

### Serviço de Autenticação Federada

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

# Problemas corrigidos

Os seguintes problemas foram corrigidos 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 falhar ao redirecionar para a sessão virtual.
- Para redirecionamento de webcam, o cliente RDP para o segundo salto não é suportado.
- Ao digitalizar uma imagem em uma sessão de desktop com o ambiente configurado conforme descrito abaixo, a imagem pode não ser digitalizada. Este problema é intermitente.
    - Instalação do driver do scanner e do aplicativo de imagem.
    - Política de redirecionamento 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
- O lançamento de um segundo aplicativo contínuo falha se o SSL estiver ativado e a confiabilidade da sessão estiver desativada. Se um aplicativo contínuo for iniciado, o lançamento subsequente de outro aplicativo contínuo para o mesmo servidor deve ser iniciado 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 broker. .
- 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 ambos os canais em ambos os ouvidos.

## Delivery Controller™

- As atualizações na tabela `MonitorData.ResourceUtilization` no banco de dados de monitoramento estão atrasadas.
- Ao usar um VDA versão 2203 CU3 com Windows 10, o instalador do VDA não hospeda a porta WCF personalizada se o Rendezvous Proxy estiver configurado.

### Director

- Ao usar um VDA de desktop de sessão única ou multissessão em um **Site de Várias Florestas**, o recurso de pesquisa centrado no usuário não funciona.

### Gráficos

- Para Windows 11 versão 22H2, ao mover uma janela do Windows Media Player dentro de uma sessão, apenas a metade inferior do vídeo é exibida. Como solução alternativa, selecione: Configurações > Sistema > Multitarefas > Ajustar janelas > Mostrar layouts de ajuste quando eu arrastar uma janela para a parte superior da minha tela
- Ao usar o Citrix Virtual Apps and Desktops 2203, você pode observar uma tela preta ao reconectar-se às sessões desconectadas.

### Política

- Após atualizar o Citrix Virtual Apps and Desktops da versão 1912 LTSR CU3 para a versão CU4 ou CU5, os VDAs podem não se registrar com o Delivery Controller e permanecer não registrados.
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA.

### Studio

- 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.
- Ao usar *Citrix Studio* e *Web Studio* em sua implantação, você pode encontrar: se você criar uma pasta de aplicativo no *Citrix Studio*, mas não adicionar nenhum aplicativo a ela, essa pasta vazia não aparece no *Web Studio*.
- 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**, você pode receber um erro. Para resolver o problema, permita cookies de terceiros no navegador.
- Ao adicionar o endereço do servidor StoreFront™ via Citrix Studio e atribuí-lo a um Grupo de Entrega, a loja é definida como desativada por padrão.

## Servidor de Impressão Universal

### Impressão

- Ao usar o VDA versão 1912 CU5 e o SO versão 2012 R2, vários trabalhos de impressão estão falhando no servidor de impressão Citrix UPS de produção com a seguinte mensagem de erro: `CCgpStream::Open: WaitForMultipleObjects time out.` `InternalUpcRemoteOpenStream: Failed to Open Stream. Abort Job.`
- Ao usar o UPS versão 2212 ou 2305 no Citrix Virtual Apps and Desktops versão 2212 ou 2305 com Windows 10 VDA, as impressoras que usam CUPS exibem a seguinte mensagem: `Access Denied, cannot connect message`

## VDA para SO de sessão única

- Ao usar o VDA do Windows, você pode encontrar um erro de mapeamento de teclado ao alternar do teclado japonês para o coreano.
- Os valores `SaveRsopToFile`, `SaveRsopToMemory` e `SaveRsopToRegistry` sob a chave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` podem não ser restaurados.
- Depois de atualizar um VDA para a versão 2203, o aplicativo Skype for Business pode parar de responder na tela inicial.
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA.
- Um deadlock no Broker Agent impede que as máquinas se registrem novamente em uma alteração de IP DNS.
- 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 na máquina ao instalar ou atualizar componentes principais.
- O processo `WebSocketService.exe` falha ao iniciar após uma reinicialização do VDA.
- Ao usar 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`
- Ao usar uma máquina, o lançamento da sessão do usuário falha intermitentemente.
- Durante uma reconexão de sessão ICA®, a janela de bate-papo de um aplicativo de mensagens de terceiros pode aparecer automaticamente em primeiro plano.

- O processo `Wfshell.exe` pode falhar ao copiar e colar arquivos de uma estação de trabalho local para a sessão Citrix para VDA LTSR 2203.
- Ao usar um VDA Windows 10 versão 2308, o processo `ctxappvservice.exe` pode falhar.
- A cópia de conteúdo de um aplicativo Microsoft Visio ou Visio publicado em um desktop para um aplicativo no dispositivo do usuário pode falhar.
- O WebSocketService (Serviço WebSocker de Redirecionamento de Vídeo HTML5) pode falhar.
- Um aplicativo definido na metade esquerda do monitor esquerdo aparece incorretamente no centro da tela após a reconexão ao usar Virtual Apps and Desktops 2203 LTSR, aplicativo Citrix Workspace™ 2203 LTSR CU3 (2303 ou 2205) e VDA 2203 LTSR com Windows 11 22h2.

### VDA para SO multissessão

- O processo `WebSocketService.exe` pode consumir mais memória do que o esperado nos VDAs.
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA.
- Um deadlock no Broker Agent impede que as máquinas se registrem novamente em uma alteração de IP DNS.
- O processo `WebSocketService.exe` falha ao iniciar após uma reinicialização do VDA.
- Ao usar uma versão VDA 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`
- Alguns processos do aplicativo Citrix Workspace podem não fechar conforme o esperado quando executados em uma sessão de aplicativo publicado.
- Na versão VDA LTSR 2203 CU3 do Server 2019, `WmiPrvSE.exe` falha.
- O processo `Wfshell.exe` pode falhar ao copiar e colar arquivos de uma estação de trabalho local para a sessão Citrix para VDA LTSR 2203.
- O processo de Serviços de Terminal pode falhar após uma reconexão ACR.
- No Windows Server 2022, se um mouse for movido para uma posição dedicada pelo aplicativo ou SO, você não poderá mover o mouse para a posição novamente até que o mouse seja movido para outro local pelo aplicativo ou SO.
- A caixa de diálogo **Mensagem de Expiração do Tempo Ocioso de Aviso** não aparece na sessão ICA no VDA do SO 2022, embora o limite de tempo de **Sessão Ociosa** entre em vigor.

- A cópia de conteúdo de um aplicativo Microsoft Visio ou Visio publicado em um desktop para um aplicativo no dispositivo do usuário pode falhar.

### Gerenciamento de Perfis

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### VDA Linux

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Gravação de Sessão

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Workspace Environment Management™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Citrix Provisioning™

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

### Serviço de Autenticação Federada

Para obter informações sobre os problemas corrigidos, consulte o artigo Problemas corrigidos em seu próprio documento.

# Problemas conhecidos

## Observações

- Os problemas conhecidos descritos nas seções de lançamento inicial 2402 e CU1 deste artigo continuam presentes no CU2, 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 seguinte aviso se aplica a qualquer solução alternativa que sugira a alteração de uma entrada de registro:

**Aviso:**

A edição incorreta do registro pode causar 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. Certifique-se de fazer backup do registro antes de editá-lo.

## Problemas conhecidos no 2402 CU4

- Ao atualizar licenças no Studio baseado em MMC, com o DDC configurado para o Serviço de Ativação de Licenças (LAS), os detalhes do arquivo de licença V6 são exibidos incorretamente por um breve período. Isso afeta temporariamente a apresentação precisa das informações de licença no MMC Studio. Para mitigar, feche e reabra o MMC Studio.

## Problemas conhecidos no 2402 CU3

- A atualização do CVAD 2402 LTSR CU3 para 2411 pode falhar. Como solução alternativa, você pode atualizar para versões mais recentes, como 2503 e superiores.
- Ao atualizar para o VDA 2402 CU3, a política Secure HDX™ é atualizada para permitida a partir de seu estado desabilitado padrão anterior.
- Ao usar o redirecionamento de conteúdo do navegador em tela cheia com várias guias, você pode ver a janela de visualização do navegador saltando enquanto uma guia é arrastada lentamente para fora. A janela de visualização do navegador se ajusta à tela do navegador assim que o arrasto é interrompido.
- Ao usar o redirecionamento de vídeo HTML5, você pode não ver os controles de vídeo para vídeos que não são reproduzidos automaticamente, embora estejam disponíveis.

## Problemas conhecidos no 2402 CU2

- O menu da bandeja do sistema do Outlook pode aparecer, mas clicar com o botão direito nele não exibe nenhum menu de ação no primeiro logon após iniciar e fazer login no aplicativo Outlook. Como solução alternativa, você pode fazer logoff e fazer login novamente na sessão para acessar o menu.
- Você pode enfrentar problemas com a janela de configurações após iniciar o aplicativo contínuo, onde o botão de fechar ('X') se separa da janela e permanece na posição inicial.
- Ao usar o pass-through de domínio aprimorado para logon único (SSO), o SSO em aplicativos dentro da sessão funciona conforme o esperado quando um usuário se conecta pela primeira

vez. No entanto, se o usuário se desconectar e depois se reconectar à mesma sessão, o SSO dentro da sessão pode parar de funcionar. Isso se deve a uma regressão introduzida com as atualizações do Windows lançadas em março e abril de 2025. Os clientes que enfrentam esse problema são aconselhados a abrir um caso de suporte com a Microsoft e referenciar o ID de rastreamento 2410230030007977.

## Problemas conhecidos no 2402 CU1

- O recurso Virtual Channel Dynamin Plugin Manager aparece na interface do usuário, mas não é compatível com a versão atual.
- Ao fazer login no Web Studio com o Administrador de Grupos de Entrega e o Escopo personalizado de Grupos de Entrega, você pode encontrar um erro ao tentar excluir uma Tag de uma máquina de SO de sessão única ou de uma máquina de várias sessões selecionando Gerenciar Tags.
- Após atualizar o StoreFront 2402 para 2402 CU1, os usuários de dispositivos em alemão podem não conseguir fazer login no aplicativo Citrix Workspace e no cliente web do Citrix Workspace em navegadores. A página de login pode carregar sem resultado. Para obter mais informações, consulte CTX691873.

## Problemas conhecidos na versão inicial 2402

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

> **Aviso:**
>
> A edição incorreta do registro 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. Certifique-se de fazer backup do registro antes de editá-lo.

## Geral

- Se o Citrix Files para Windows e/ou Citrix Files para Office estiverem 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.

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

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

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

- Em alguns cenários, ao usar o filtro de política de IP do Cliente, o endereço IP usado para avaliar a política está incorreto.
- Ao usar o pass-through de domínio aprimorado para logon único, o SSO na sessão pode falhar se o dispositivo cliente ou o host da sessão estiver executando o Windows 11.
- 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.
- Devido aos novos recursos relacionados ao App-V adicionados no CVAD 2311, a funcionalidade do App-V agora é totalmente suportada apenas no Web Studio. O uso do MMC Studio para App-V pode levar a problemas.

a. Aplicativos App-V existentes podem parar de funcionar

Após atualizar o Delivery Controller (DDC) para: 2402 LTSR CU3 ou versões anteriores do 2402 LTSR, ou 2507 RTM, Os aplicativos App-V criados anteriormente usando o MMC Studio podem não funcionar como esperado. Como solução alternativa: Para 2402 LTSR CU3 ou versões anteriores do 2402 LTSR, execute sql no siteDB :

```
-- Convert Broker Apps which are Packaged Apps to be explicitly
labeled as such.

-- this is detected by the presence of ctxAppVLauncher.exe on the
command line

-- The application record in the Applibrary and the related Package
and Library denote which packaging technology was used.



    update chb_Config.Applications

    set ApplicationType = 4, --$ATPackagedApplication

        --NB: The AppLibrary's LibaryUid and the Broker's
PackagedApplicationType have the same value

        PackagedApplicationType = case
```

```
                                    when
TRY_CONVERT(uniqueidentifier, A.CommandLineArguments) is null then 2
--Dual Admin

                                    else 1 -- Single Admin.

                                            -- This is a bug with
legacy MMC Studio not understanding the new Broker App format. But
only App-V apps can be affected

                                end,

        PackagedApplicationId = case

                                    when
TRY_CONVERT(uniqueidentifier, A.CommandLineArguments) is null then
REPLACE(A.CommandLineArguments, N'"','')

                                    else CONVERT(char(36),
CONVERT(uniqueIdentifier,  A.CommandLineArguments))

                                end

    from chb_Config.Applications A

        inner join chb_Config.ApplicationsMetadata AMD on A.Uid =
AMD.ApplicationUid

    where A.CommandLineExecutable like N'%ctxAppVLauncher.exe'

        and A.ApplicationType = 0 --$ATHostedOnDesktop

        and AMD.Name = 'Citrix_DesktopStudio_SequenceLocation'

        and right(AMD.Value, 5) = '.appv'
```

b. Criando Novos Aplicativos App-V no MMC Studio

No 2402 LTSR e 2507 LTSR, a criação de novos aplicativos App-V via MMC Studio pode não funcionar corretamente. Recomenda-se usar o Web Studio para criar novos aplicativos App-V.

## Políticas

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

## Gráficos

- Se você iniciar uma pré-visualização de vídeo usando um aplicativo de webcam de 64 bits com compressão Theora, a sessão pode travar.
- Você pode notar webcams extras conectadas à área de trabalho remota no aplicativo Skype para desktop. A visualização dessas webcams extras é bloqueada e pode mostrar uma tela preta por motivos de segurança. Você pode ignorar a webcam extra e continuar usando a webcam do endpoint.
- H265 444 em GPUs Intel e algumas NVIDIA pode resultar em artefatos visíveis na sessão. Para problemas relacionados a GPUs Intel, há uma solução temporária para redimensionar a sessão ou alternar o modo de tela cheia.

## Machine Creation Services™

- Em um ambiente VMware hospedado na AWS, a criação do catálogo de máquinas MCS falha se a imagem mestre estiver com vTPM habilitado. Esse problema afeta todas as versões do Citrix Virtual Apps and Desktops e é devido a um problema no ambiente VMware. Para obter assistência, entre em contato com o suporte VMware.
- Ao atualizar um site Multi-Delivery Controller de algumas versões LTSR pré-2402 (incluindo as versões 2302, 2305, 2308, 2311) para o 2402 LTSR, as ações de energia em uma VM podem falhar se o site estiver apenas parcialmente atualizado. 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 apenas no Windows 10. Para obter mais informações, consulte CTX213540.
- A impressora padrão pode não ser marcada corretamente na janela de diálogo de impressão. Esse problema não afeta os trabalhos de impressão enviados para a impressora padrão.

- Alguns trabalhos de impressão de impressoras de rede com balanceamento de carga podem falhar quando as conexões SSL para os Universal Print Servers estão habilitadas. Isso acontece quando os trabalhos de impressão são disparados rapidamente um após o outro.
- **A impressão pode falhar após uma atualização in-loco do Windows em máquinas com o Citrix VDA já instalado** Após uma atualização in-loco do Windows, os provedores de impressão Citrix podem não ser mais invocados, o que pode resultar em falhas de impressão. Esse problema ocorre porque o processo de atualização do Windows redefine a ordem de execução do provedor de impressão e não preserva os provedores registrados da Citrix. A Microsoft confirmou que este é um comportamento do Windows e atualmente não preserva os registros de provedores na ordem de execução durante as atualizações.

A solução alternativa é adicionar os provedores de impressão de volta ao local apropriado do registro.

```
1.  Open the Registry Editor.

1.  Go to `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Print\Providers`

1.  Right-click **order** and select **Modify**.

1.  Add the values `Universal Printer` and `Client Printer` above any
other providers.

1.  Reboot the VDA.
```

## FIDO2

- Ao usar um navegador baseado em Chromium em sua sessão de aplicativo virtual ou desktop, o registro da chave FIDO2 não funciona se o navegador estiver executando a versão 147 do Chromium ou mais recente.

A atualização para a versão 2503 do VDA ou mais recente resolve esse problema.

Alternativamente, como solução alternativa, você pode desabilitar o redirecionamento FIDO2 e usar o redirecionamento USB para redirecionar a chave FIDO2 para a sessão. Para obter detalhes, consulte redirecionamento USB.

## Problemas de terceiros

- O Chrome oferece suporte à Automação da Interface do Usuário apenas para barras de ferramentas, guias, menus e botões ao redor de uma página da web. Devido a esse problema

do Chrome, o recurso de exibição automática do teclado pode não funcionar em um navegador Chrome em dispositivos de toque. Como solução alternativa, execute `chrome --force-renderer-accessibility` ou você pode abrir uma nova guia do navegador, digitar `chrome://accessibility` e habilitar o suporte à **API de acessibilidade nativa** para páginas específicas ou todas as páginas. Além disso, ao publicar um aplicativo contínuo, você pode publicar o Chrome com a opção `--force-renderer-accessibility`.

- Você pode ver uma tela preta ao iniciar uma sessão se tiver o FSLogix 2201 HF1 instalado no host da sessão. Para resolver esse problema, você deve atualizar o FSLogix para uma versão mais recente.

## Gerenciamento de Perfis

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

## VDA Linux

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

## Gravação de Sessão

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

## Workspace Environment Management™

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

## Citrix Provisioning™

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

## Serviço de Autenticação Federada

- Para obter informações sobre os problemas conhecidos, consulte o artigo Problemas conhecidos em seu próprio documento.

# Descontinuações e remoções

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

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

## Descontinuações

Descontinuação significa que pretendemos remover o recurso ou a capacidade de uma versão futura. O recurso ou a capacidade continuará funcionando e será totalmente suportado até ser oficialmente removido. Esta notificação de descontinuação pode durar alguns meses ou anos. Após a remoção, o recurso ou a capacidade não funcionará mais. Este aviso serve para permitir tempo suficiente para você planejar e atualizar seu código antes que o recurso ou a capacidade seja removido. Alternativas para itens descontinuados são sugeridas sempre que possível.

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| Plug-in de terceiros do HPE Moonshot Machine Manager | 2402 | Use o plug-in HPE Moonshot gerenciado pela Citrix |
| Licenciamento baseado em arquivo | 2507 | License Activation Service (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. Os clientes que usam licenciamento |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| | | baseado em arquivo são obrigados a atualizar para uma versão compatível e realizar esta transição tecnológica antes de April 15, 2026. O LAS será a única forma de ativar e licenciar componentes locais da Citrix após April 15, 2026. |
| Rendezvous V1 | 2402 | Use o Rendezvous V2. |
| Secure ICA® | 2402 | Use o Secure HDX. |
| Suporte a VDA no Windows Server 2016 | 2402 | Atualize para as versões mais recentes do Windows Server. |
| Suporte para Delivery Controller™, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI para SO de sessão única, VDA para SO de múltiplas sessões, floresta e domínio do Active Directory e Universal Print Server no | 2402 | Atualize para a versão mais recente do Windows Server. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| Windows Server 2016 | | |
| Suporte para as versões 2016 e 2017 do Microsoft SQL Server para os bancos de dados de configuração do site, registro de configuração e monitoramento | 2402 | Atualize para a versão mais recente do Microsoft SQL Server. |
| Suporte para configurar o cache de write-back para incluir apenas um cache de disco e nenhum cache de memória | 2402 | Use a opção de configuração de 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 "legados") | 2402 | Recrie as VMs de catálogo herdadas do Azure. Os catálogos são provisionados sob demanda e, assim, economizam custos de armazenamento. |
| A política de **Taxa de Quadros Mínima Alvo** | 2311 | Use o **Indicador de Status Gráfico** para modificar a taxa de quadros mínima alvo. |
| Suporte para Citrix Connector 3.1 para System Center | 2311 | Faça a atualização da imagem ou do |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| Configuration Manager | | aplicativo manualmente. |
| Suporte para usar uma imagem mestre em uma região diferente da região onde o catálogo é criado | 2311 | Use a Galeria de Computação do Azure para replicar a imagem mestre para a região desejada. |
| Configuração do limite de memória de exibição gráfica HDX™ | 2311 | A quantidade mínima de memória necessária é alocada para garantir que o layout de exibição do cliente seja totalmente acomodado. |
| Suporte ao modo progressivo em HDX Graphics | 2311 | Use o Thinwire. Consulte Modo progressivo. |
| Suporte para redirecionamento de conteúdo do navegador no Internet Explorer 11 | 2311 | Use o redirecionamento de conteúdo do navegador baseado no Google Chrome. |
| Removido o suporte para o worker de volume do AWS | 2311 | Use o upload e download direto de disco. Consulte Upload e download direto de disco. |
| Suporte para SQL Server 2016 no Broker | 2308 | Use as versões mais recentes. Para obter mais informações, |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| | | consulte Requisitos do sistema. |
| Suporte para XenApp 5.x no Director | 2308 | --- |
| Suporte para XenApp 6.x no Director | 2308 | --- |
| Pacote SCOM para alertas no Director | 2308 | --- |
| Suporte para plug-in no Director | 2308 | --- |
| Suporte para formato WebRTC SDP (Plano B) | 2308 | Atualize o Citrix Workspace™ App para uma versão compatível. |
| Suporte para o modo de Janela Única na Otimização do Microsoft Teams | 2308 | Atualize o Citrix Workspace App para uma versão que suporte o modo MultiWindow. Para obter mais informações, consulte Matriz de recursos e suporte de versão. |
| Suporte para `AwsCaptureInstanceProperties` usado em ambientes AWS | 2308 | Use um perfil de máquina. Consulte Criar um catálogo usando um perfil de máquina. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| `Schedule-ProvVMUpdate` comando PowerShell | 2305 | Use `Set-ProvVMUpdateTimeWindow`. |
| `Request-ProvVMUpdate` comando PowerShell | 2305 | Use `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`. |
| `Cancel-ProvVMUpdate` comando PowerShell | 2305 | Use `Clear-ProvVMUpdateTimeWindow`. |
| Parâmetro `DedicatedTenancy` usado no comando `New-ProvScheme` | 2303 | Use o parâmetro `TenancyType`. |
| License Server VPX | 2206 | --- |
| Redirecionamento de Host para Cliente (URL) | 2203 | Redirecionamento de conteúdo bidirecional. |
| Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-Hypsecuritygroupegress` e `Grant-HypSecurityGroupIngress` usados em | 2203 | --- |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| ambientes de nuvem e locais. | | |
| Citrix Files para Windows e Citrix Files para Outlook do metainstalador do VDA. | 2203 | Use os instaladores autônomos. |
| Componente do Agente WEM do metainstalador do VDA. | 2203 | --- |
| Opção Wake on LAN integrada ao SCCM para Acesso Remoto a PC. | 2012 | Use o recurso Wake on LAN autônomo. |
| Suporte para o assistente de importação PVS no Citrix Studio | 1912 LTSR | Provisionar máquinas Citrix Provisioning usando uma das seguintes formas:<br>• Provisione máquinas usando o Citrix Provisioning Console e exporte-as para o Citrix Virtual Apps and Desktops usando o Assistente de Exportação de |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | ALTERNATIVA |
|---|---|---|
| | | Dispositivos do Citrix Provisioning. Consulte Assistente de Exportação de Dispositivos para mais detalhes. |
| Citrix SCOM Management Packs para XenApp e XenDesktop, Provisioning Services e StoreFront. Para as versões de produto que podem ser monitoradas, consulte a documentação do Citrix SCOM Management Packs. | 1912 | Use o Director para monitorar e gerenciar sua implantação. Para mais informações sobre o EOL do SCOM e alternativas, consulte https://support.citrix.com/article/CTX266943. |
| Mobility SDK / Mobile SDK (dos antigos Citrix Labs) | 7.16 | Substituído pelas configurações de política de experiência móvel e experiências nativas para desktops/ aplicativos hospedados. |

## Remoções

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

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Citrix Workspace app para Windows 1912 | --- | 2402 | Use as versões mais recentes. |
| Otimização de gráficos HDX em tela cheia + texto | 2311 | 2311 | |
| Suporte para NVIDIA Frame Buffer Capture (NVFBC) com HDX 3D Pro | 2308 | 2311 | Use a API de Duplicação de Área de Trabalho (DDAPI). |
| Suporte VDA para a configuração de política "Instalação automática de drivers de impressora incluídos". | 7.16 | 2311 | Nenhum. Configuração de política suportada apenas com VDAs em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores). |
| Codificação de hardware de GPU NVIDIA (NVENC) com: vGPU 11 e anteriores, e versão de driver 466.77 e anteriores. | 2305 | 2305 | Use os drivers NVIDIA atualmente suportados: vGPU 13 ou mais recente, versão 471.41 ou mais recente. |
| Ferramentas de Suporte Citrix (SupportabilityTool_x | --- | 2212 | --- |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| 64 .msi) do Meta-Instalador VDA. | | | |
| Citrix License Administration Console (última inclusão 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 VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR. |
| Codificação de hardware com GPUs NVIDIA (NVENC) usando drivers de vídeo GRID 9 ou anteriores. | 2003 | 2003 | Use drivers de vídeo GRID 10 com VDAs do Citrix Virtual Apps and Desktops 7 2003 ou posterior, ou use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR. |
| Recurso de Redefinição de Senha de Autoatendimento (SSPR). | 2003 | 2006 | --- |
| Suporte para versões do Microsoft .NET | 1912 | 2003 | Atualize para a versão 4.8 do .NET Framework. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Framework anteriores à versão 4.8 para VDAs e componentes principais do servidor. Inclui Delivery Controller, Studio e Director. | | | |
| VDAs no Windows Server 2012 R2. | 1912 | 2003 | Instale VDAs em um sistema operacional compatível. |
| Componente de migração de aplicativos AppDNA® da edição Citrix Virtual Apps and Desktops Premium. | 1909 | 2003 | --- |
| Instalando o Studio em máquinas de 32 bits (x86). | 1909 | 2003 | Instale em um sistema operacional x64 compatível. |
| Suporte para o hook do Excel em aplicativos contínuos. Isso era 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 | 1906 | 2003 | Instale em um sistema operacional |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Service Packs). Inclui: Delivery Controller, Studio e Director. | | | compatível mais recente. |
| Suporte para bancos de dados de Configuração de Site, Registro de Configuração e Monitoramento em versões do Microsoft SQL Server 2008 R2, 2012 e 2014 (incluindo todos os Service Packs e edições). | 1906 | 2003 | Instale bancos de dados em uma versão compatível do Microsoft SQL Server. |
| Suporte para VDAs no Windows 10 em plataformas x86. | 1906 | 1909* | Instale VDAs em um sistema operacional x64 compatível. *Este recurso ainda é compatível 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- | 1903 | 1903 | --- |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Box e XenMobile (9.0 e anteriores). | | | |
| Suporte para Linux VDA no Red Hat Enterprise Linux/ CentOS 7.5. | 1903 | 1903 | Instale o Linux VDA em uma versão posterior do Red Hat Enterprise Linux. |
| Suporte do StoreFront para 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 os Citrix Receivers para um aplicativo Citrix Workspace que suporte o protocolo TLS 1.2. Para obter mais informações sobre o aplicativo Citrix Workspace, consulte (/pt-br/citrix-workspace-app). |
| Suporte VDA para a configuração de política "Instalação automática de drivers de impressora integrados". | 7.16 | 2311 | Nenhum. Configuração de política suportada apenas com VDAs 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 Desktop Lock para casos de uso não associados a domínio. |
| Suporte para a tecnologia de acesso | 1811 | 1903 | Use Thinwire com transporte adaptável ativado. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| remoto de exibição Framehawk | | | |
| Suporte para Citrix Smart Scale em todas as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Esta funcionalidade atingirá o Fim da Vida Útil em 31 May 2019. | 1808 | 1906 | Considere usar o Virtual Apps and Desktops Service no Citrix Cloud para funcionalidade aprimorada 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 em uma versão SUSE compatível. |
| Suporte para o driver Citrix WDDM em VDAs | 7.16 | 7.16 | O driver Citrix WDDM não é mais instalado com VDAs. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| VDAs no Windows 10 versão 1511 (Threshold 2) e versões anteriores do Windows Single-session OS, incluindo Windows 8.x e Windows 7 (consulte `<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>`). | 7.15 LTSR (e 7.12) | 7.16 | Instale VDAs de SO de sessão única no Windows 10 versão mínima 1607 (Redstone 1) ou em Canais Semestrais mais recentes. Se estiver usando 1607 LTSB, recomendamos um VDA 7.15. Consulte CTX224843. |
| VDAs no Windows Server 2008 R2 e Windows Server 2012 (incluindo Service Packs) | 7.15 LTSR (e 7.12) | 7.16 | Instale VDAs em um sistema operacional compatível. |
| Redirecionamento de Composição da Área de Trabalho (anteriormente conhecido como DirectX Command Remoting) (DCR) | 7.15 LTSR | 7.16 | Use Thinwire. |
| Experiência clássica do Citrix Receiver for Web (interface de usuário de “bolhas verdes”) | 7.15 LTSR (e StoreFront 3.12) | 1903 | Experiência unificada do Citrix Receiver for Web. |

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

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| | | | sites públicos. Para obter mais informações, consulte a nota Fim da Vida Útil do Redirecionamento Flash. |
| Integração Citrix Online (produto Goto) com StoreFront | 7.14 (e StoreFront 3.11) | StoreFront 3.12 | --- |
| A conta de usuário, CtxAppVCOMAdmin, que foi criada durante a instalação do VDA e adicionada ao Grupo de Administradores Locais na máquina VDA, não é mais criada. O mecanismo "COM" subjacente também foi removido. | 7.14 | 7.14 | O serviço Windows CtxAppVService executa a mesma função. Ele é instalado e configurado automaticamente e não requer interação do usuário. |
| Suporte ao componente UpsServer do Universal Print Server no Windows Server 2008 de 32 bits | 7.14 | 7.14 | Instale em um sistema operacional mais recente e compatível. |
| StoreFront e Receiver for Web no Internet Explorer 8 | 7.13 | 7.13 | --- |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Opção de instalação de linha de comando do VDA /no_appv para evitar a instalação dos componentes do Citrix App-V | 7.13 | 7.13 | Use a opção de instalação de linha de comando / exclude "Citrix Personalization for App-V – VDA". |
| O instalador completo do produto não instala mais o snap-in Citrix.Common.Commands em novas instalações e o remove automaticamente ao atualizar instalações existentes. | 7.13 | 7.13 | Alguns comandos do PowerShell que eram fornecidos pelo snap-in Citrix.Common.Commands ainda estão disponíveis no SDK do XenApp 6.5. |
| Funcionalidade parcial para manipular dados de ícones que era fornecida pelos *-CtxIcon cmdlets. | 7.13 | 7.13 | Agora fornecido pelos *-BrokerIcon cmdlets no Serviço Broker. |
| Modo Thinwire herdado | 7.12 | 7.16 | Use Thinwire. 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. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| Upgrades in-loco do StoreFront 2.0, 2.1, 2.5 e 2.5.2 | 7.13 | 7.16 | Faça upgrade de uma dessas versões para uma versão posterior compatível e depois para o XenApp e XenDesktop 7.16. |
| Upgrades in-loco 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 faça upgrade para o XenDesktop 7.6 LTSR (com o CU mais recente) e, em seguida, faça upgrade para a versão mais recente do Citrix Virtual Desktops (anteriormente XenDesktop) ou versão 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. |
| Concessão de conexão | 7.12 | 7.16 | Use Cache de Host Local. |

| ITEM | DESCONTINUAÇÃO ANUNCIADA NA VERSÃO | REMOVIDO NA VERSÃO | ALTERNATIVA |
|---|---|---|---|
| XenDesktop 5.6 usado no Windows XP. Instalações de VDA no Windows XP não são suportadas. | 7.12 | 7.16 | Instale VDAs em um sistema operacional compatível. |
| Suporte para conexões CloudPlatform | 7.12 | 2003 | Use um hipervisor ou serviço de nuvem compatível diferente. |
| Suporte para conexões do Azure Classic (também conhecido como Azure Service Management) | 7.12 | 2003 | Considere usar o Serviço Virtual Apps and Desktops no Citrix Cloud. |
| Funcionalidade AppDisks (e a integração do AppDNA no Studio, que a suporta) | 7.13 | 2003 | Use o Citrix App Layering. |
| Funcionalidade Personal vDisk | 7.15 | 2006† | Use a tecnologia de camada de usuário do Citrix App Layering ou camada 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

## Introdução

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

Revise Preparar para instalar antes de iniciar uma instalação.

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

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

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

### Requisitos de hardware

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

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

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

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

### Dimensionamento de VMs que entregam desktops e aplicativos

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

Para mais informações:

- Citrix Tech Zone contém orientações sobre dimensionamento.
- Escalabilidade de Servidor Único do Citrix Virtual Apps and Desktops discute quantos usuários ou VMs podem ser suportados em um único host físico.

## Microsoft Visual C++

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

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

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

## Delivery Controller

Sistemas operacionais suportados:

- Windows Server 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 Redistributable.
- Se você atualizar do Citrix Virtual Apps and Desktops versão 2407 para 2411 ou posterior, ou realizar uma nova instalação da versão 2411 ou posterior, atualize o License Server para a versão mais recente (versão 11.2.17 build 53100 ou posterior) como primeira etapa. Em seguida, atualize o Delivery Controller. Não fazer isso resultará em uma mensagem de aviso na interface do usuário e falha nas instalações por linha de comando.

## Bancos de dados

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

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

- SQL Server 2016 SP2, edições Express, Standard e Enterprise.

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

- Instâncias de Cluster de Failover SQL Server AlwaysOn
- Grupos de Disponibilidade SQL Server AlwaysOn (incluindo Grupos de Disponibilidade Básicos)
- Espelhamento de Banco de Dados SQL Server

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

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

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

**Mais informações sobre o banco de dados:**

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

# Web Studio

> **Observação:**

- Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.
- O Web Studio é um console de gerenciamento baseado na web que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. Ele foi projetado para uma experiência de usuário aprimorada e geralmente responde mais rápido do que o Citrix Studio, o console de gerenciamento baseado em Windows. Consulte Instalar o Web Studio.

Sistemas operacionais suportados:

- 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 suportados:

- 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 Conteúdo Estático instalado. Se este software ainda não estiver instalado, você será solicitado a fornecer a mídia de instalação do Windows Server. Em seguida, esse software é instalado para você.

- Para visualizar os logs de eventos em máquinas onde o Citrix Director está instalado, você deve instalar o Microsoft .NET Framework 2.0.

Citrix Profile Management:

- Certifique-se de que o Citrix Profile Management e o Plug-in WMI do Citrix Profile Management estejam instalados no VDA (página **Componentes Adicionais** no assistente de instalação) e que o Serviço Citrix Profile Management esteja em execução para visualizar os detalhes do perfil do usuário no Director.

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

- System Center 2012 R2 Operations Manager

Navegadores compatíveis para visualizar o Director:

- 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 suportados:

- Windows 11
- Windows 10 (somente x64), qualquer versão que esteja atualmente em suporte mainstream.
    - Para suporte a edições, 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 Redistributable.

O Remote PC Access usa este VDA, que você instala em PCs físicos de escritório. Este VDA oferece suporte ao Secure Boot para Citrix Virtual Desktops™ Remote PC Access no Windows 11 e Windows 10.

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

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

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

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

## Virtual Delivery Agent (VDA) para SO multissessão

Sistemas operacionais suportados:

- Windows 11 (suportado apenas com Citrix DaaS™)
- Windows 10 (somente x64; compatível apenas com Citrix DaaS), qualquer versão que esteja atualmente em suporte mainstream.
- Windows Server 2022
- Windows Server 2019, Standard e Datacenter Editions
- Windows Server 2016, Standard e Datacenter Editions

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

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

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

Vários recursos de aceleração multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado na máquina onde você instala o VDA. Se a máquina não tiver o Media Foundation instalado, os recursos de aceleração multimídia não serão instalados e não funcionarão. Não remova o Media Foundation da máquina após instalar o software Citrix; caso contrário, os usuários não conseguirão fazer logon na máquina. Na maioria das versões do Windows Server, o recurso Media Foundation é instalado através do Gerenciador do Servidor. Para obter mais informações, consulte Preparar para instalar.

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

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

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

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

## Hosts / recursos de virtualização

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

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

O recurso Remote PC Access Wake on LAN requer o Microsoft System Center Configuration Manager mínimo 2012.

Hypervisores suportados:

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

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

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

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

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

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

- **Nutanix Acropolis**

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

  Para obter mais informações, consulte Nutanix virtualization environments.

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

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

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

  Para obter mais informações, consulte VMware virtualization environments.

Hosts de nuvem pública suportados:

- **Amazon Web Services (AWS)**

  Para obter informações sobre como usar o AWS para provisionar máquinas virtuais, consulte Amazon Web Services virtualization environments.

- **Google Cloud Platform** Para obter mais informações, consulte Google Cloud Platform virtualization environments e Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

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

- **Soluções de nuvem e parceiros Nutanix**

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

- **Soluções de nuvem e parceiros VMware**

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

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

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

## Níveis funcionais do Active Directory

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

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

> **Observação:**

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

# HDX

## Áudio

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

O cancelamento de eco é compatível com o 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.

## Entrega de mídia HDX Windows

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

## HDX 3D Pro

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

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

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

  - Microsoft Hyper-V no Windows Server 2016, onde é referido como Atribuição de Dispositivo Discreto (DDA).

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

Consulte `<https://docs.citrix.com/pt-br/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 de 2,3 GHz ou superior.

Unidade de Processamento Gráfico (GPU):

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

Dispositivo do usuário:

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

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

## Servidor de Impressão Universal

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

O componente UpsServer é suportado em:

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

Requisitos:

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

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

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

Para obter mais informações, consulte Provisionar impressoras.

## Outro

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

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

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

O Microsoft Group Policy Management Console (GPMC) é necessário se você armazenar informações de política do Citrix no Active Directory em vez do banco de dados de configuração do site. Se você instalar `CitrixGroupPolicyManagement_x64.msi` separadamente (por exemplo, em uma máquina que não tenha um componente principal do Citrix Virtual Apps and

Desktops instalado), essa máquina deve ter o tempo de execução do Visual Studio 2015 instalado. Para obter mais informações, consulte a documentação da Microsoft.

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

Múltiplas 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 Aplicativos Locais para obter informações sobre navegadores suportados para esse recurso.

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

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

# Visão geral técnica

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

Citrix Virtual Apps and Desktops permitem:

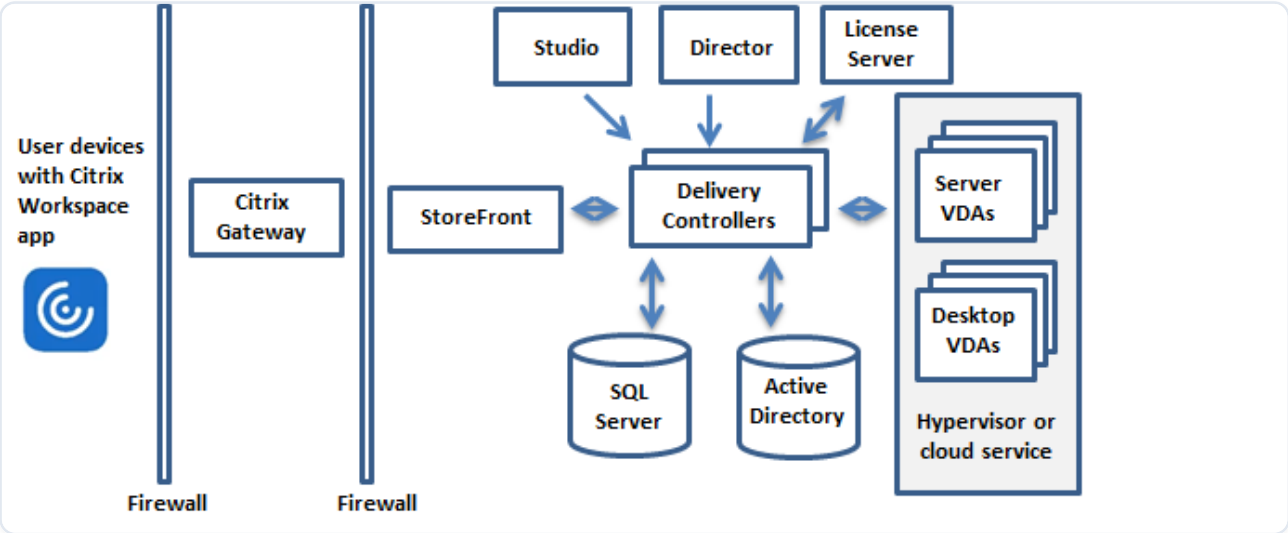
- Que os usuários finais executem aplicativos e desktops independentemente do sistema operacional e da interface do dispositivo.
- Que os administradores gerenciem a rede e controlem o acesso de dispositivos selecionados ou de todos os dispositivos.
- Que os administradores gerenciem uma rede inteira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

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

## Componentes principais

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

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




## Delivery Controller™

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

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

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

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

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

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

## Banco de dados

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

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

## Agente de Entrega Virtual (VDA)

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

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

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

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

## Citrix StoreFront™

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

## Aplicativo Citrix Workspace™

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

## Studio

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

### Web Studio

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

### Citrix Studio

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

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

## Acesso Privado Seguro

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

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

## Citrix Director

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

O Director exibe:

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

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

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

## Servidor de Licenças Citrix

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

## Hypervisor ou outro serviço

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

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

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

# Componentes adicionais

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

## Citrix Provisioning™

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

## Citrix Gateway

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

## Citrix SD-WAN™

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

# Como funcionam as implantações típicas

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

Comunicações de componentes em uma implantação(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/deployment-overview.png)

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

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

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

# Como as conexões de usuário são tratadas

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

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

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

Fluxo de conexão do usuário(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/user-connections.png)

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

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

O Controller envia uma mensagem ao VDA com as credenciais do usuário e, em seguida, envia todos os dados sobre o usuário e a conexão para o VDA. O VDA aceita a conexão e envia as informações de volta pelos mesmos caminhos para o aplicativo Citrix Workspace. Um conjunto de parâmetros necessários é coletado no StoreFront. Esses parâmetros são então enviados ao aplicativo Citrix Workspace como parte da conversa do protocolo Citrix-Workspace-app-StoreFront, ou convertidos em um arquivo Independent Computing Architecture (ICA) e baixados. Desde que o site tenha sido configurado corretamente, as credenciais permanecem criptografadas durante todo este processo.

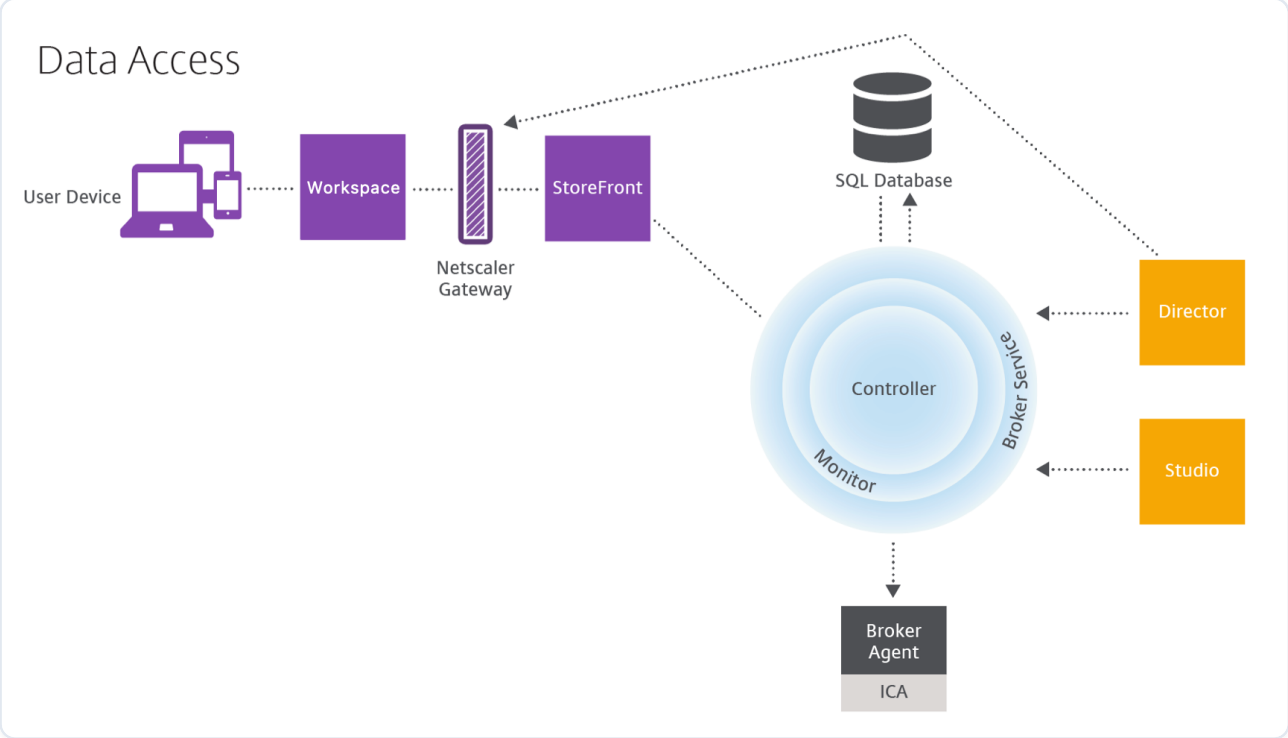
O arquivo ICA é copiado para o dispositivo do usuário e estabelece uma conexão direta entre o dispositivo e a pilha ICA em execução no VDA. Esta conexão ignora a infraestrutura de gerenciamento (aplicativo Citrix Workspace, StoreFront e Controller).

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

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

## Como o acesso a dados funciona

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




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

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

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

# Entregar desktops e aplicativos

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

## Catálogos de máquinas

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

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

Os tipos de máquina válidos são:

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

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

## Grupos de entrega

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

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

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

Para obter mais informações, consulte Criar grupos de entrega.

### Grupos de aplicativos

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

Para obter mais informações, consulte Criar grupos de aplicativos.

## Mais informações

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

## Bancos de dados

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

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

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

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

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

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

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

## Alta disponibilidade

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

- **Grupos de Disponibilidade AlwaysOn (incluindo Grupos de Disponibilidade Básicos):** Esta solução de alta disponibilidade e recuperação de desastres de nível empresarial, introduzida no SQL Server 2012, permite maximizar a disponibilidade para um ou mais bancos de dados. Os Grupos de Disponibilidade AlwaysOn exigem que as instâncias do SQL Server residam em nós do Windows Server Failover Clustering (WSFC). Para obter mais informações, consulte Windows Server Failover Clustering com SQL Server.
- **Espelhamento de banco de dados SQL Server:** O espelhamento do banco de dados garante que, se você perder o servidor de banco de dados ativo, um processo de failover automático ocorra em questão de segundos, de modo que os usuários geralmente não sejam afetados. Este método é mais caro do que outras soluções porque licenças completas do SQL Server são necessárias em cada servidor de banco de dados. Você não pode usar a edição SQL Server Express em um ambiente espelhado.
- **Clustering SQL:** A tecnologia de clustering do Microsoft SQL pode ser usada para permitir automaticamente que um servidor assuma as tarefas e responsabilidades de outro servidor que falhou. No entanto, configurar essa solução é mais complicado, e o processo de failover automático é tipicamente mais lento do que alternativas como o espelhamento SQL.
- **Usando os recursos de alta disponibilidade do hipervisor:** Com este método, você implanta o banco de dados como uma máquina virtual e usa os recursos de alta disponibilidade do seu hipervisor. Esta solução é menos dispendiosa do que o espelhamento porque usa o seu software de hipervisor existente e você também pode usar a edição SQL Server Express. No entanto, o processo de failover automático é mais lento, pois pode levar tempo para uma nova máquina iniciar para o banco de dados, o que pode interromper o serviço para os usuários.

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

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

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

## Instalar software de banco de dados

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

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

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

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

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

Use o Windows Update para manter o SQL Server atualizado.

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

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

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

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

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

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

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

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

### Configuração automática

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

Se um banco de dados existir no endereço especificado, ele deve estar vazio. Se os bancos de dados não existirem em um endereço especificado, você será informado de que um banco de dados não pode ser encontrado e, em seguida, perguntado se deseja que o banco de dados seja criado para você. Ao confirmar essa ação, o Web Studio cria automaticamente os bancos de dados e, em seguida, aplica os scripts de inicialização para os bancos de dados principal e de réplica.

### Configuração por script

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

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

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

Você pode indicar onde armazenar os scripts.

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

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

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

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

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

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

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

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

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

## Permissões necessárias para configurar bancos de dados

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

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

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

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

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

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

### Scripts de direitos de banco de dados preferenciais

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

Usando o PowerShell, você pode especificar os direitos de banco de dados preferenciais. A especificação de um valor não padrão resulta na criação de scripts separados. Um script contém tarefas que precisam da função `securityadmin`. O outro script requer apenas direitos

`db_owner` e pode ser executado por um administrador Citrix, sem ter que contatar um administrador de banco de dados.

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

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

Para obter mais informações, consulte a ajuda do cmdlet.

## Formatos de endereço de banco de dados

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

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

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

Para espelhamento de banco de dados, especifique apenas o endereço do servidor principal. O Citrix Site Manager localiza o servidor espelho com base no servidor principal.

Para obter mais informações sobre como configurar o SQL Server autônomo, o Espelhamento de Banco de Dados e o Always On High Availability, consulte este artigo CTX.

## Alterar locais do banco de dados

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

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

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

Para alterar o local de um banco de dados:

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

### Mais informações

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

## Métodos de entrega

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

## Introdução

A escolha do método de entrega de aplicativos apropriado ajuda a melhorar a escalabilidade, o gerenciamento e a experiência do usuário.

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

Para desktops, considere desktops publicados ou desktops VDI.

## Aplicativos e desktops publicados do Citrix Virtual Apps™

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

**Caso de uso:**

- Você deseja uma entrega baseada em servidor de baixo custo para minimizar o custo de entrega de aplicativos a muitos usuários, ao mesmo tempo em que oferece uma experiência de usuário segura e de alta definição.
- Seus usuários executam tarefas bem definidas e não exigem personalização ou acesso offline a aplicativos. Os usuários podem incluir trabalhadores de tarefas, como operadores de call center e trabalhadores de varejo, ou usuários que compartilham estações de trabalho.
- Tipos de aplicativo: qualquer aplicativo.

**Benefícios e considerações:**

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

**Experiência do usuário:**

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

**Processar, hospedar e entregar aplicativos:**

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

**Gerenciamento e atribuição de sessão:**

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

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

## Aplicativos hospedados em VM

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

**Caso de uso:**

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

**Benefícios e considerações:**

- Aplicativos e desktops na imagem mestre são gerenciados, hospedados e executados com segurança em máquinas dentro do seu data center, fornecendo uma solução de entrega de aplicativos mais econômica.

- No logon, os usuários podem ser atribuídos aleatoriamente a uma máquina dentro de um grupo de entrega configurado para hospedar o mesmo aplicativo. Você também pode atribuir estaticamente uma única máquina para entregar um aplicativo a um único usuário cada vez que esse usuário faz logon. Máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de várias sessões não é suportada em máquinas de SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega ao fazer logon, e os usuários devem estar online para acessar seus aplicativos.
- Este método pode aumentar a quantidade de recursos do servidor para processar aplicativos e aumentar a quantidade de armazenamento para os dados dos usuários.

**Experiência do usuário:**

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

**Processar, hospedar e entregar aplicativos:**

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

**Gerenciamento e atribuição de sessão:**

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

## Desktops VDI

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

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

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

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

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

## Acesso Remoto ao PC

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

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

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

Para obter mais informações, Acesso Remoto a PC.

# Portas de rede

Informações completas sobre portas de rede são fornecidas em Portas de Comunicação Usadas pelas Tecnologias Citrix.

Quando os componentes Citrix® são instalados, o firewall do host do sistema operacional também é atualizado, por padrão, para corresponder às portas de rede padrão.

Você pode precisar de informações de porta:

- Para conformidade regulatória.
- Se houver um firewall de rede entre os componentes do Citrix Virtual Apps and Desktops™ e outros produtos ou componentes Citrix, para que você possa configurar esse firewall adequadamente.
- Se você usar um firewall de host de terceiros, como um fornecido com um pacote anti-malware, em vez do firewall do host do sistema operacional.
- Se você alterar a configuração do firewall do host nesses componentes (geralmente Windows Firewall Service).
- Se você reconfigurar os recursos do componente para usar uma porta ou intervalo de portas diferente e, em seguida, quiser desabilitar ou bloquear portas que não são usadas em sua configuração.

Algumas das portas são registradas na Internet Assigned Numbers Authority (IANA). Detalhes sobre essas atribuições estão disponíveis em `<http://www.iana.org/assignments/port-numbers>`. No entanto, as informações descritivas mantidas pela IANA nem sempre refletem o uso atual.

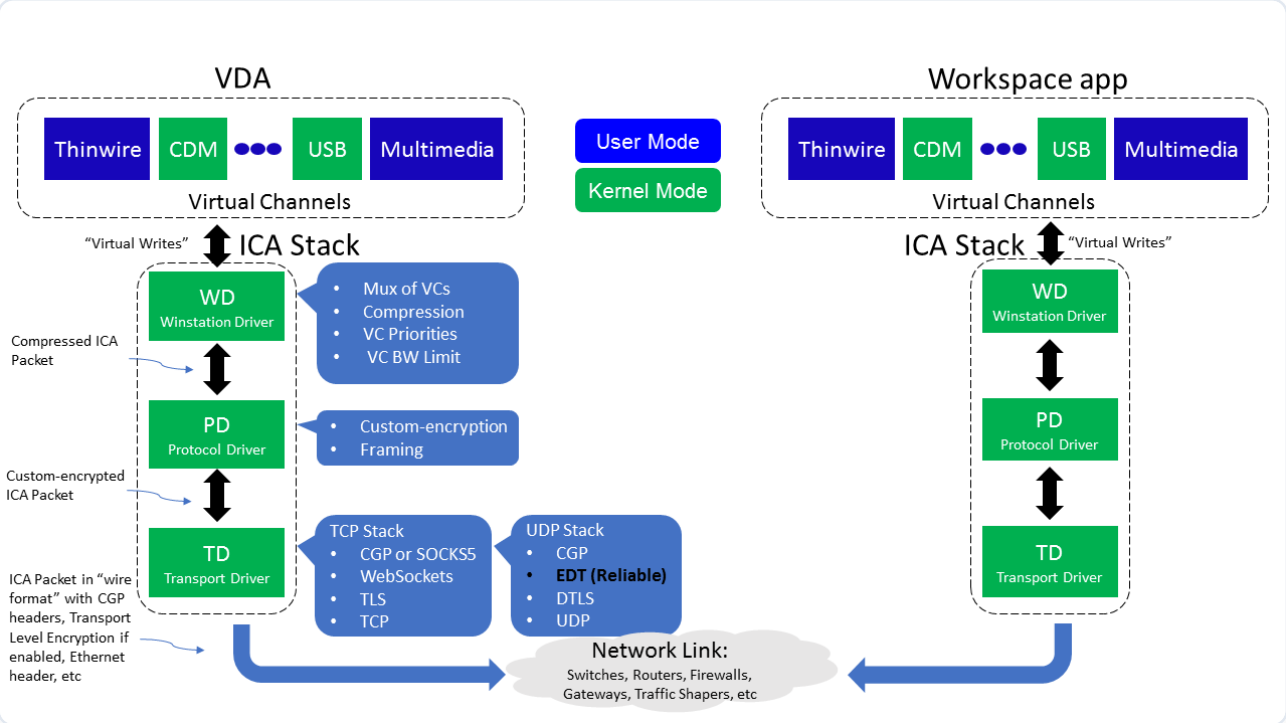
Além disso, os sistemas operacionais no VDA e no Delivery Controller™ exigem portas de entrada para seu próprio uso. Consulte a documentação do Microsoft Windows para obter detalhes.

## HDX™

> **Aviso:**

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

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



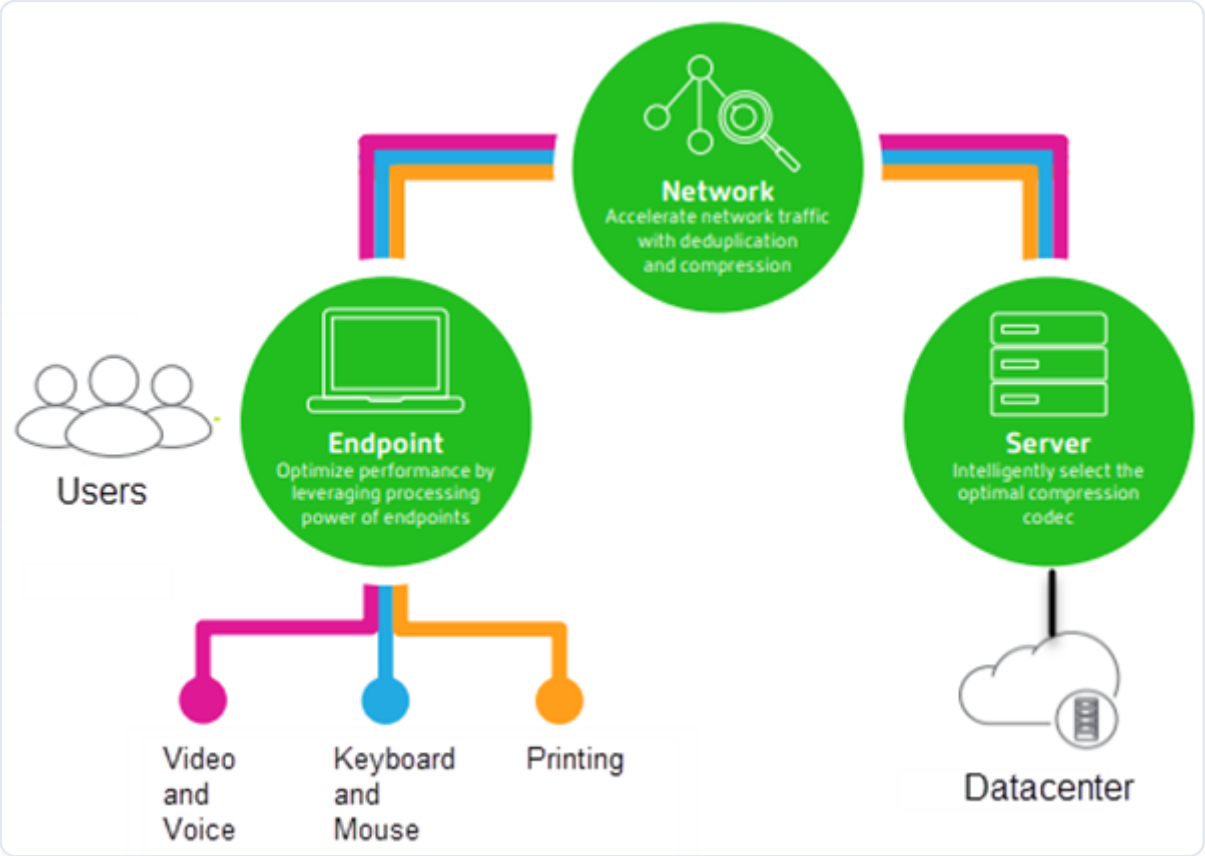

O HDX foi projetado com base em três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

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

- **Redirecionamento inteligente** - O redirecionamento inteligente examina a atividade da tela, os comandos do aplicativo, o dispositivo de endpoint e os recursos de rede e servidor para determinar instantaneamente como e onde renderizar uma atividade de aplicativo ou desktop. A renderização pode ocorrer no dispositivo de endpoint ou no servidor de hospedagem.

- **Compressão adaptativa** - A compressão adaptativa permite que exibições multimídia ricas sejam entregues em conexões de rede finas. O HDX primeiro avalia várias variáveis, como o tipo de entrada, dispositivo e exibição (texto, vídeo, voz e multimídia). Ele escolhe o codec de compressão ideal e a melhor proporção de uso de CPU e GPU. Em seguida, ele se adapta inteligentemente com base em cada usuário e base únicos. Essa adaptação inteligente é por usuário, ou mesmo por sessão.




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

Para obter mais informações, consulte Aumente a produtividade com um espaço de trabalho de usuário de alta definição.

## No dispositivo

O HDX usa a capacidade de computação dos dispositivos do usuário para aprimorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários recebam uma experiência

suave e contínua com conteúdo multimídia em seus desktops ou aplicativos virtuais. O controle de espaço de trabalho permite que os usuários pausem desktops e aplicativos virtuais e retomem o trabalho de um dispositivo diferente no ponto em que pararam.

## Na rede

O HDX incorpora recursos avançados de otimização e aceleração para oferecer o melhor desempenho em qualquer rede, incluindo conexões WAN de baixa largura de banda e alta latência.

Os recursos do HDX se adaptam às mudanças no ambiente. Os recursos equilibram desempenho e largura de banda. Eles aplicam as melhores tecnologias para cada cenário de usuário, seja o desktop ou aplicativo acessado localmente na rede corporativa ou remotamente de fora do firewall corporativo.

## No data center

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

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

## HDX Insight

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

Você pode habilitar o NetScaler para usar o canal virtual HDX Insight para mover todos os pontos de dados necessários em um formato não compactado. Se você desabilitar esse recurso, o dispositivo NetScaler descriptografa e descompacta o tráfego ICA® espalhado por vários canais virtuais. Usar o canal virtual único diminui a complexidade, aumenta a escalabilidade e é mais econômico.

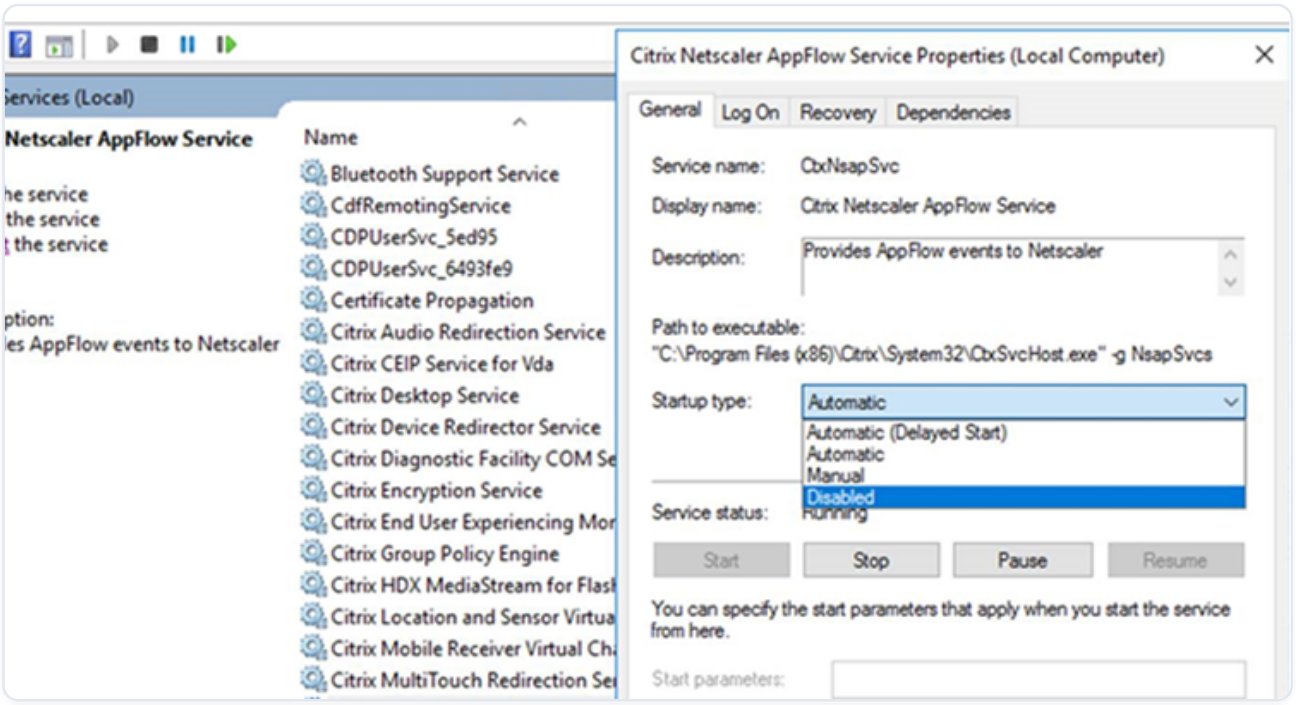
**Requisitos mínimos:**

- NetScaler versão 12.0 Build 57.x
- Citrix Workspace™ app para Windows 1808

- Citrix Receiver para Windows 4.10
- Citrix Workspace app para Mac 1808
- Citrix Receiver para Mac 12.8

### Habilitar ou desabilitar o canal virtual HDX Insight

Para desabilitar este recurso, defina as propriedades do serviço Citrix NetScaler Application Flow como Desabilitado. Para habilitar, defina o serviço como Automático. Em ambos os casos, recomendamos que você reinicie a máquina do servidor após alterar essas propriedades. Por padrão, este serviço está habilitado (Automático).




## Experimente os recursos HDX do seu desktop virtual

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

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

  b. Para experimentar como o redirecionamento de conteúdo do navegador acelera a entrega de conteúdo multimídia para desktops virtuais, assista a um vídeo em seu desktop a partir de um site que contenha vídeos HTML5, como o YouTube. Os usuários não sabem quando o redirecionamento de conteúdo do navegador está em execução. Para ver se o redirecionamento de conteúdo do navegador está sendo usado, arraste a janela do navegador rapidamente. Você verá um atraso ou fora do quadro entre a janela de visualização e a interface do usuário. Você também pode clicar com o botão direito do

mouse na página da web e procurar por **Sobre o Redirecionamento de Navegador HDX** no menu.

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

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

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

Por padrão, o HDX oferece uma experiência superior de gráficos e vídeo para a maioria dos usuários, e a configuração não é necessária. As configurações de política do Citrix que proporcionam a melhor experiência para a maioria dos casos de uso são habilitadas por padrão.

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

É bom saber:

- Para obter informações de suporte e requisitos para recursos HDX, consulte o artigo Requisitos do sistema. Salvo indicação em contrário, os recursos HDX estão disponíveis para máquinas Windows Multi-session OS e Windows Single-session OS compatíveis, além de desktops de Acesso Remoto para PC.
- Este conteúdo descreve como otimizar a experiência do usuário, melhorar a escalabilidade do servidor ou reduzir os requisitos de largura de banda. Para obter informações sobre como usar políticas e configurações de política do Citrix, consulte a documentação Políticas do Citrix para esta versão.

- Para instruções que incluem a edição do registro, use com cautela: editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

## Reconexão automática do cliente e confiabilidade da sessão

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

**Reconexão automática do cliente:**

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

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

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

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

Configurações padrão de reconexão automática do cliente:

- Tempo limite de reconexão automática do cliente: 120 segundos
- Reconexão automática do cliente: Ativada
- Autenticação de reconexão automática do cliente: Desativada
- Registro de reconexão automática do cliente: Desativado

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

**Confiabilidade da sessão:**

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

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

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

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

Configurações padrão de confiabilidade da sessão

- Tempo limite de confiabilidade da sessão: 180 segundos
- Nível de opacidade da interface do usuário de reconexão: 80%
- Conexão de confiabilidade da sessão: Habilitado
- Número da porta de confiabilidade da sessão: 2598

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

**NetScaler com reconexão automática do cliente e confiabilidade da sessão:**

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

- A confiabilidade da sessão está desabilitada no NetScaler Gateway.

- Ocorre um failover no dispositivo NetScaler.
- O NetScaler SD-WAN é usado com o NetScaler Gateway.

## Taxa de transferência adaptativa HDX

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

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

> **Importante:**

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

> Este recurso tem os seguintes requisitos:

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

## Melhorar a qualidade da imagem enviada para os dispositivos do usuário

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

- Qualidade visual. Controla a qualidade visual das imagens exibidas no dispositivo do usuário: média, alta, sempre sem perdas, construir para sem perdas (padrão = média). A qualidade real do vídeo usando a configuração padrão de média depende da largura de banda disponível.
- Taxa de quadros alvo. Especifica o número máximo de quadros por segundo que são enviados do desktop virtual para o dispositivo do usuário (padrão = 30). Para dispositivos com CPUs

mais lentas, especificar um valor menor pode melhorar a experiência do usuário. A taxa de quadros máxima suportada por segundo é 60.

- Limite de memória de exibição. Especifica o tamanho máximo do buffer de vídeo para a sessão em kilobytes (padrão = 65536 KB). Para conexões que exigem maior profundidade de cor e resolução mais alta, aumente o limite. Você pode calcular a memória máxima necessária.

**Observação:**

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

## Melhorar o desempenho da videoconferência

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

Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**. Para impedir que os usuários alternem da compactação de vídeo da webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em Configurações de política ICA > Configurações de política de dispositivos USB.

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

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

Se uma webcam suportar codificação de hardware, a compactação de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compactação de software, adicione o seguinte valor de chave DWORD à chave do registro: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

## Prioridades de tráfego de rede

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

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

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

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

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

> **Aviso:**

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

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

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

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

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

## Mostrar ou ocultar a barra de idiomas remota

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

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

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

## Mapeamento de teclado Unicode

Os Citrix Receivers não Windows usam o layout de teclado local (Unicode). Se um usuário alterar o layout de teclado local e o layout de teclado do servidor (código de varredura), eles podem não estar sincronizados e a saída estará incorreta. Por exemplo, o Usuário1 altera o layout de teclado

local de inglês para alemão. O Usuário1 então altera o teclado do lado do servidor para alemão. Mesmo que ambos os layouts de teclado sejam alemães, eles podem não estar sincronizados, causando uma saída de caracteres incorreta.

### Habilitar ou desabilitar o mapeamento de layout de teclado Unicode

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

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

### Habilitar o modo compatível de mapeamento de layout de teclado Unicode

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valor: 1

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

# Canais virtuais Citrix ICA®

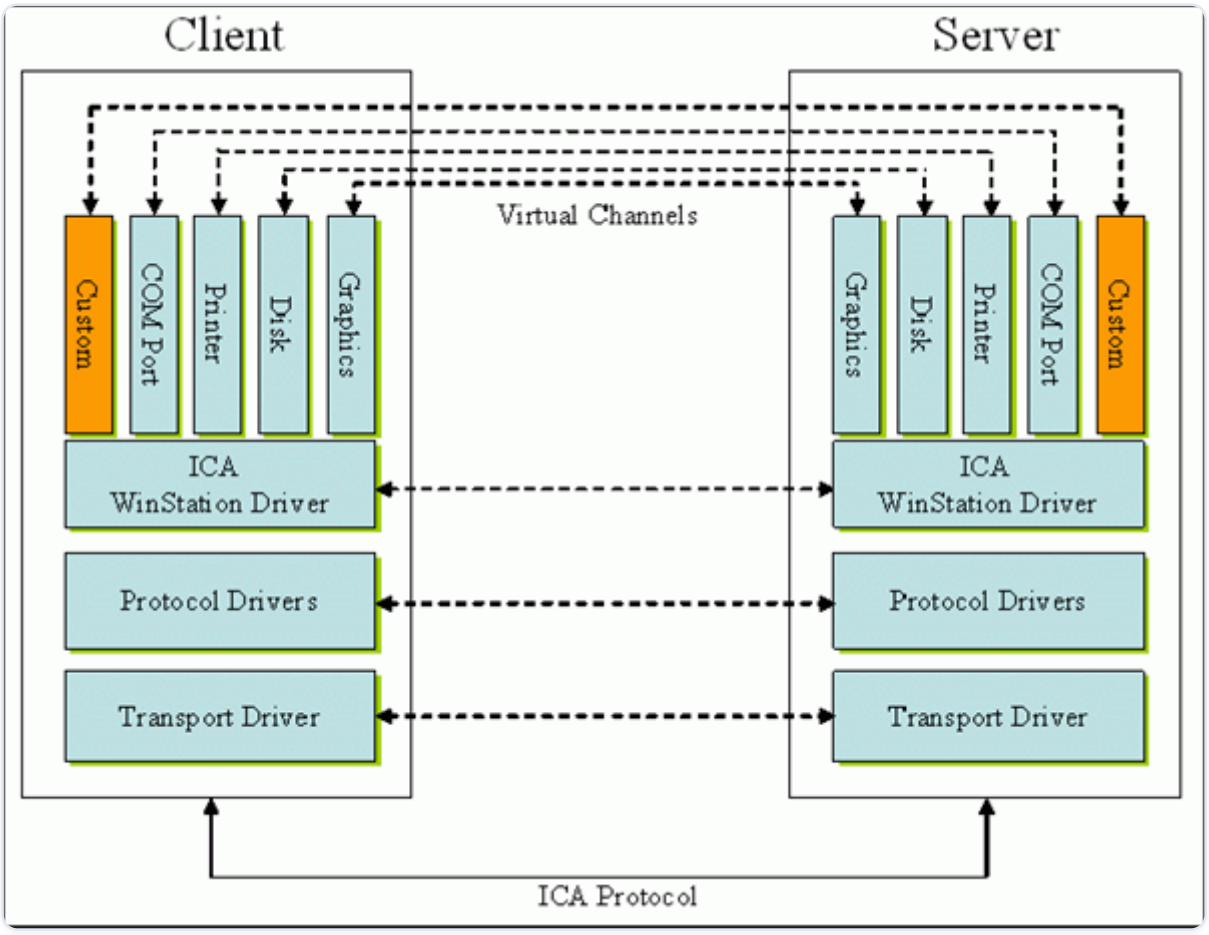
> **Aviso:**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco.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

## O que são canais virtuais ICA?

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

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

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




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

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

No lado do cliente, os canais virtuais correspondem a drivers virtuais. Cada driver virtual fornece uma função específica. Alguns são necessários para a operação normal, e outros são opcionais. Os drivers virtuais operam no nível do protocolo da camada de apresentação. Pode haver vários protocolos ativos a qualquer momento, multiplexando canais fornecidos pela camada de protocolo Windows Station (WinStation).

As seguintes funções estão contidas no valor do registro VirtualDriver sob este caminho de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

Ou

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (para 64 bits)

- Thinwire3.0 (Obrigatório)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Área de Transferência
- ClientComm
- ClientAudio
- LicenseHandler (Obrigatório)
- TWI (Obrigatório)
- SmartCard
- ICACTL (Obrigatório)
- SSPI
- TwainRdr
- Experiência do Usuário
- Vd3d

> **Observação:**

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

> Esta lista contém os arquivos de driver virtual do cliente e suas respectivas funções. O Citrix Virtual Apps e o aplicativo Citrix Workspace para Windows usam esses arquivos. Eles estão na forma de Bibliotecas de Vínculo Dinâmico (modo de usuário), e não drivers do Windows (modo kernel), exceto para USB Genérico, conforme descrito no canal virtual USB Genérico.

- vd3dn.dll – Canal virtual Direct3D usado para redirecionamento de composição de área de trabalho

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

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

### Compatibilidade de 64 bits

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

- brapi64.dll
- confmgr.dll
- ctxlogging.dll

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

### Canal virtual USB genérico

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

- ctxusbm.sys
- ctxusbr.sys

### Como os canais virtuais ICA funcionam

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

Módulos de canal virtual carregados pelo Shell, por exemplo:

- EUEM
- Twain
- Área de Transferência
- Multimídia
- Compartilhamento de sessão contínuo
- Fuso Horário

Alguns são carregados como modo kernel, por exemplo:

- CtxDvcs.sys – Canal virtual dinâmico
- Icausbb.sys – Redirecionamento USB genérico

- Picadm.sys – Mapeamento de unidade do cliente
- Picaser.sys – Redirecionamento de porta COM
- Picapar.sys – Redirecionamento de porta LPT

### Canal virtual gráfico no lado do servidor

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

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

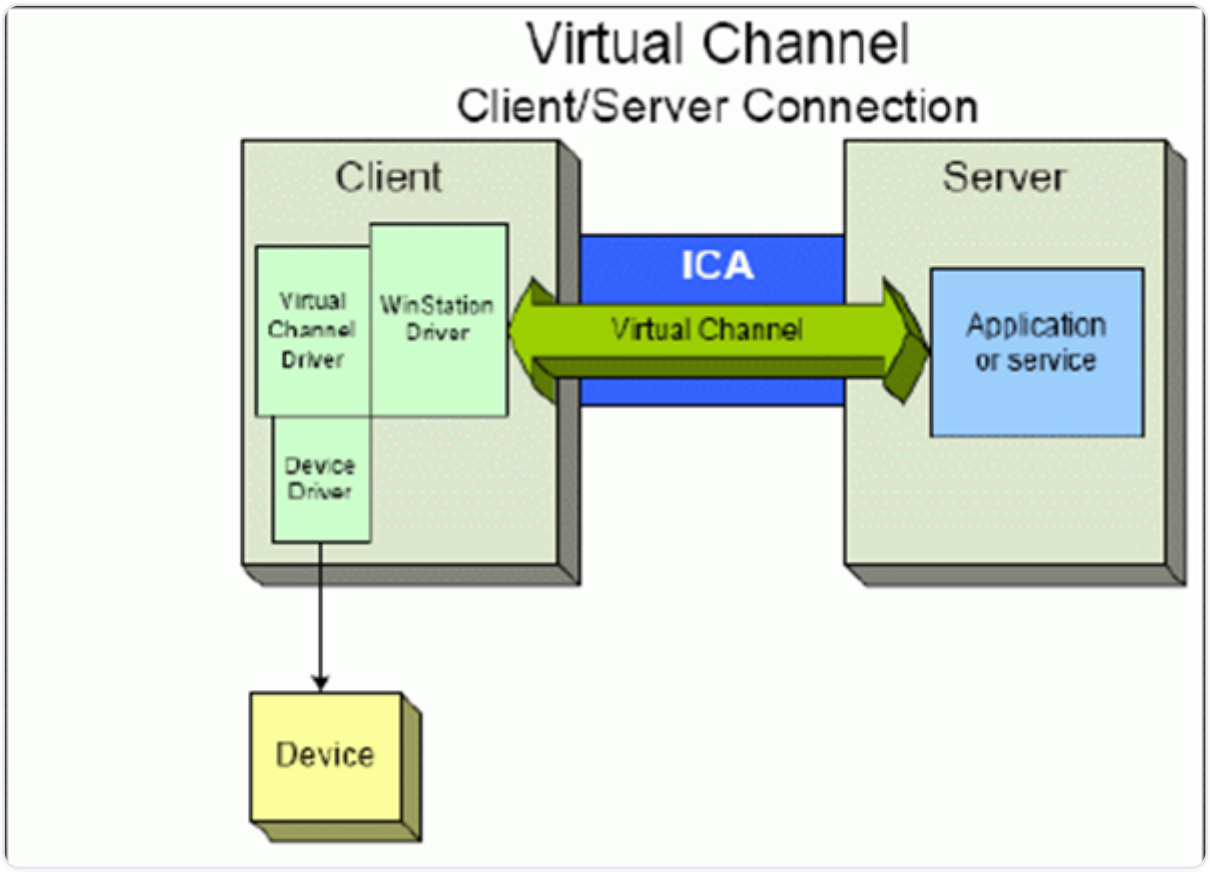
### Hospedando canais especializados em serviços do Windows

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

- Serviço de Redirecionamento de Dispositivo Citrix
- Serviço de Canal Virtual Dinâmico Citrix
- Serviço de Monitoramento da Experiência do Usuário Final Citrix
- Serviço de Canal Virtual de Localização e Sensor Citrix
- Serviço de Redirecionamento MultiToque Citrix
- Serviço de Gerenciador de Impressão Citrix
- Serviço de Smartcard Citrix
- Serviço de Redirecionamento de Áudio Citrix (somente Citrix Virtual Desktops™)
- Serviço de Canal de Status ICA Citrix

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

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




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

1. O cliente se conecta ao servidor Citrix Virtual Apps and Desktops. O cliente passa informações sobre os canais virtuais que ele suporta para o servidor.
2. O aplicativo do lado do servidor inicia, obtém um manipular para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.
3. O driver virtual do cliente e o aplicativo do lado do servidor passam dados usando os dois métodos a seguir:
    - Se o aplicativo do servidor tiver dados para enviar ao cliente, os dados serão enviados ao cliente imediatamente. Quando o cliente recebe os dados, o driver WinStation desmultiplexa os dados do canal virtual do fluxo ICA e os passa imediatamente para o driver virtual do cliente.
    - Se o driver virtual do cliente tiver dados para enviar ao servidor, os dados serão enviados na próxima vez que o driver WinStation o sondar. Quando o servidor recebe os dados, eles são enfileirados até que o aplicativo do canal virtual os leia. Não há como alertar o aplicativo do canal virtual do servidor de que os dados foram recebidos.
4. Quando o aplicativo de canal virtual do servidor é concluído, ele fecha o canal virtual e libera todos os recursos alocados.

## Criando seu próprio canal virtual usando o SDK de Canal Virtual

**Observação:**

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

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

**Observação:**

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

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

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

**Importante:**

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

## Funcionalidade de pass-through de canais virtuais

A maioria dos canais virtuais fornecidos pela Citrix opera sem modificações ao usar o aplicativo Citrix Workspace para Windows em uma sessão ICA (também conhecida como sessão de pass-through). Há considerações ao usar o cliente em saltos extras.

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

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

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

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

> **Importante:**

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

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

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

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

Oferecemos suporte aos seguintes canais virtuais tradicionais e suas funcionalidades:

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

## Segurança e canais virtuais ICA

Garantir o uso é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança localizadas em todo este documento.

## Melhores práticas

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

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

**Nomeando os Canais Virtuais:**

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

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

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

**Suporte a Double-Hop:**

| CANAL VIRTUAL | O DOUBLE HOP É SUPORTADO? |
|---|---|
| Áudio | Não |
| Redirecionamento de Conteúdo do Navegador | Não |
| CDM | Sim |
| CEIP | Não |
| Área de transferência | Sim |
| Continuum (MRVC) | Não |
| VC de Controle | Sim |
| Redirecionamento de Vídeo HTML5 (v1) | Sim |
| Teclado, Mouse | Sim |
| Multitoque | Não |
| NSAPVC | Não |
| Impressão | Sim |
| SensVC | Não |

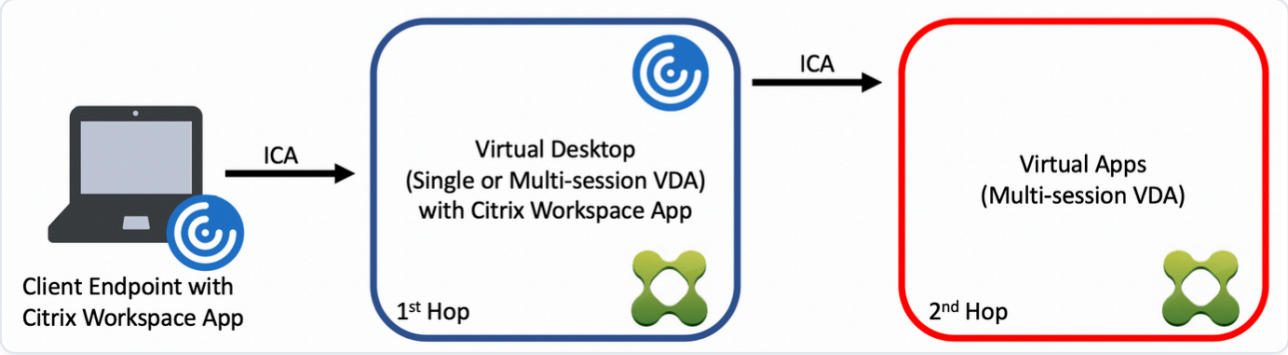
| CANAL VIRTUAL | O DOUBLE HOP É SUPORTADO? |
|---|---|
| Smartcard | Sim |
| Twain | Sim |
| VC USB | Sim |
| Dispositivos WAYCOM -K2M usando VC USB | Sim |
| Compressão de Vídeo da Webcam | Sim |
| Redirecionamento de Mídia do Windows | Sim |

## Consulte também

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

# Salto duplo em Citrix Virtual Apps and Desktops™

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




Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktop executado em um VDA de SO de sessão única (conhecido como VDI) ou em um VDA de SO de várias sessões (conhecido como desktop publicado), isso é considerado o primeiro salto. Depois que o

usuário se conecta ao desktop virtual, o usuário pode iniciar uma sessão de Citrix Virtual Apps™. Isso é considerado o segundo salto.

Você pode usar um modelo de implantação de salto duplo para oferecer suporte a vários casos de uso. O caso em que os ambientes Citrix Virtual Desktop e Citrix Virtual Apps são gerenciados por entidades diferentes é um exemplo comum. Esse método também pode ser eficaz na resolução de problemas de compatibilidade de aplicativos.

## Requisitos do sistema

Todas as edições do Citrix Virtual Apps and Desktops, incluindo o serviço Citrix Cloud™, oferecem suporte a salto duplo.

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

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

Em ambientes onde o primeiro salto envolve uma solução de desktop virtual de terceiros (não Citrix) em combinação com uma sessão de Citrix Virtual Apps, o suporte é limitado ao ambiente Citrix Virtual Apps. No caso de quaisquer problemas relacionados ao desktop virtual de terceiros, incluindo — mas não se limitando a — compatibilidade do aplicativo Citrix Workspace™, redirecionamento de dispositivos de hardware e desempenho da sessão, a Citrix pode fornecer suporte técnico em capacidade limitada. Um Citrix Virtual Desktop no primeiro salto pode ser necessário como parte da solução de problemas.

## Considerações de implantação para HDX™ em salto duplo

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

### Gráficos

Use as configurações gráficas padrão (codificação seletiva) nos primeiros e segundos saltos. No caso de HDX 3D Pro, a Citrix recomenda fortemente que todos os aplicativos que exigem

aceleração gráfica sejam executados localmente no primeiro salto com os recursos de GPU apropriados disponíveis para o VDA.

### Latência

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

### Multimídia

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

### Redirecionamento de dispositivo USB

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

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

| PRIMEIRO SALTO (VDI OU DESKTOP PUBLICADO) | SEGUNDO SALTO (APLICATIVOS VIRTUAIS) | NOTAS DE SUPORTE |
|---|---|---|
| | | suporte ao dispositivo estiver disponível. |
| Otimizado | Genérico | Não suportado |

**Nota:**

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

## Exceções de suporte

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

- Redirecionamento de conteúdo do navegador
- Acesso a aplicativos locais
- Pacote de otimização em tempo real para Skype for Business
- Otimização para Microsoft Teams

# Instalar e configurar

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

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

## Preparar

Revise Preparar para instalar e conclua todas as tarefas necessárias.

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

## Instalar componentes principais

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

## Criar um site

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

## Instalar um ou mais Virtual Delivery Agents (VDAs)

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

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

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

## Instalar componentes opcionais

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

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

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

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

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

## Criar um catálogo de máquinas

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

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

# Criar um grupo de entrega

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

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

# Criar um grupo de aplicativos (opcional)

Depois de criar um grupo de entrega, você pode opcionalmente criar um grupo de aplicativos. Você pode criar grupos de aplicativos para aplicativos que são compartilhados entre diferentes grupos de entrega ou usados por um subconjunto de usuários dentro dos grupos de entrega.

# Limitação conhecida

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

# Configurar autenticação de cartão inteligente para Web Studio

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

Etapa 1: Instalar o driver do cartão inteligente

Etapa 2: Emitir certificados para usuários de cartão inteligente

Etapa 3: Registrar certificados para usuários de cartão inteligente

Etapa 4: Configurar servidores IIS do Web Studio

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

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

> **Observação:**

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

## Etapa 1: Instalar o driver do cartão inteligente

Instale o driver do cartão inteligente nas seguintes máquinas:

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

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

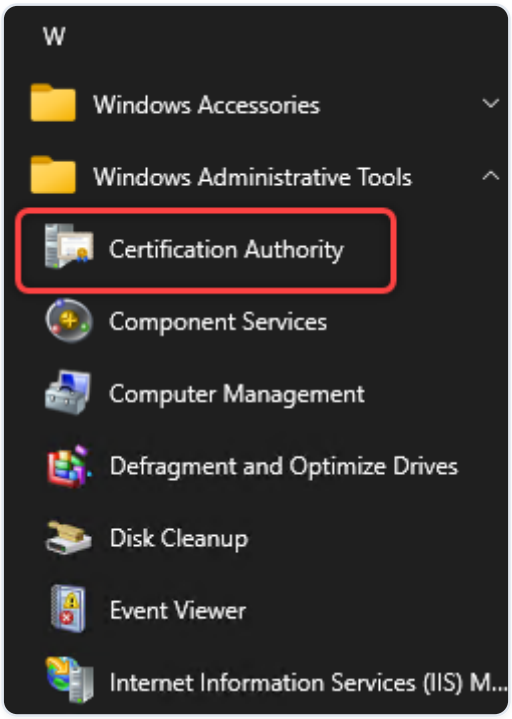
## Etapa 2: Emitir certificados para usuários de cartão inteligente

> **Observação:**

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

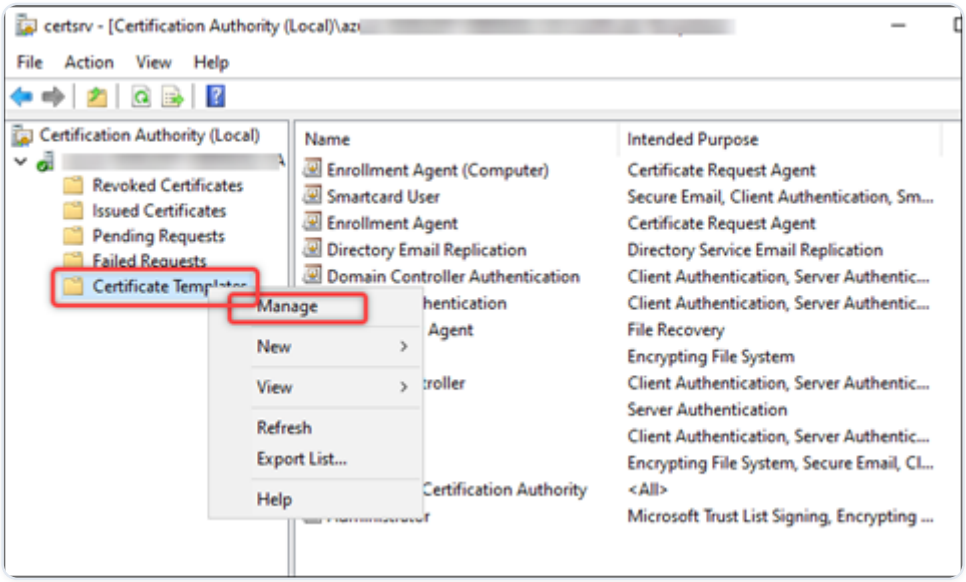
> No seu Controlador de Domínio, siga estas etapas para concluir a tarefa:

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



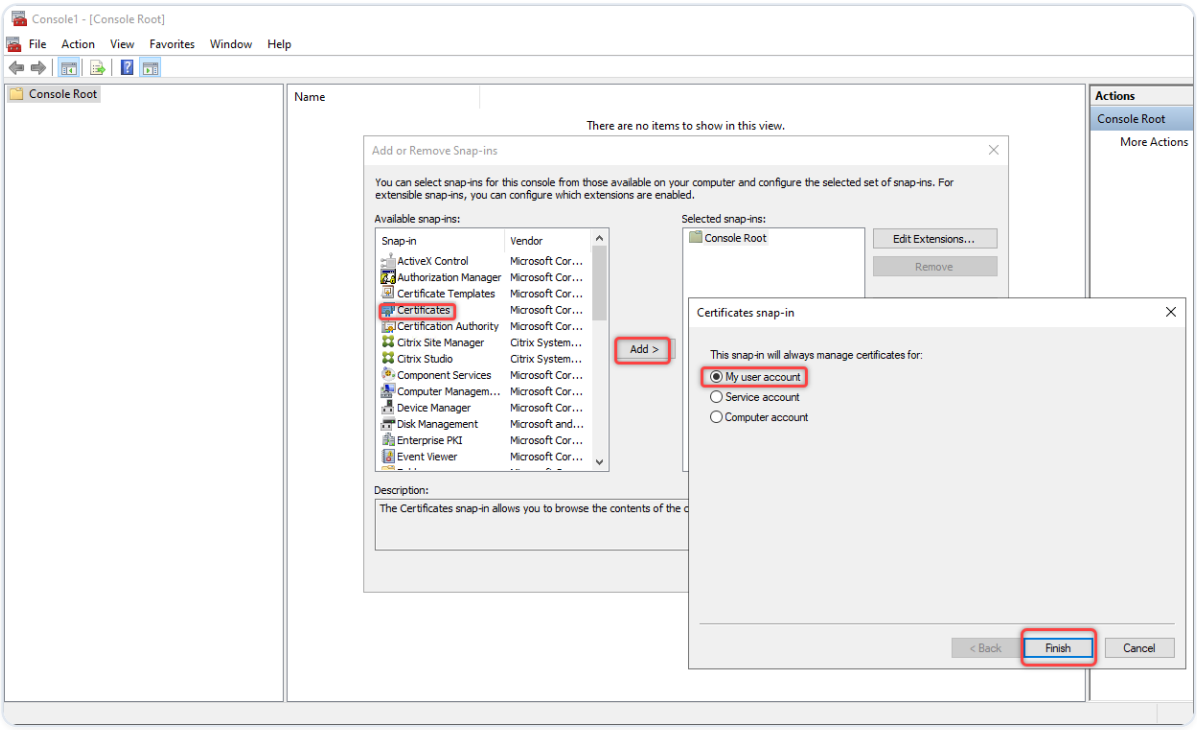

2. Duplique o modelo **Agente de Registro**. As etapas detalhadas são as seguintes:

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

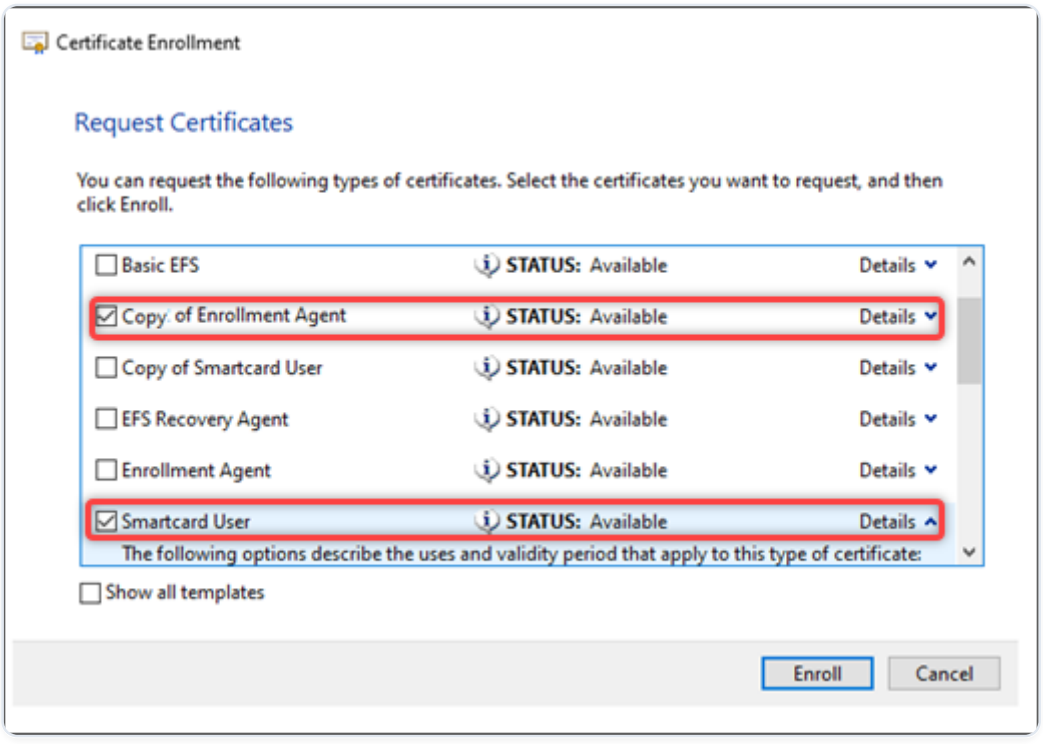



   b. Clique com o botão direito em **Agente de Registro** e selecione **Duplicar Modelo**.

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




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




3. Emita certificados para cartões inteligentes. As etapas detalhadas são as seguintes:

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

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

   c. Clique em **OK**.

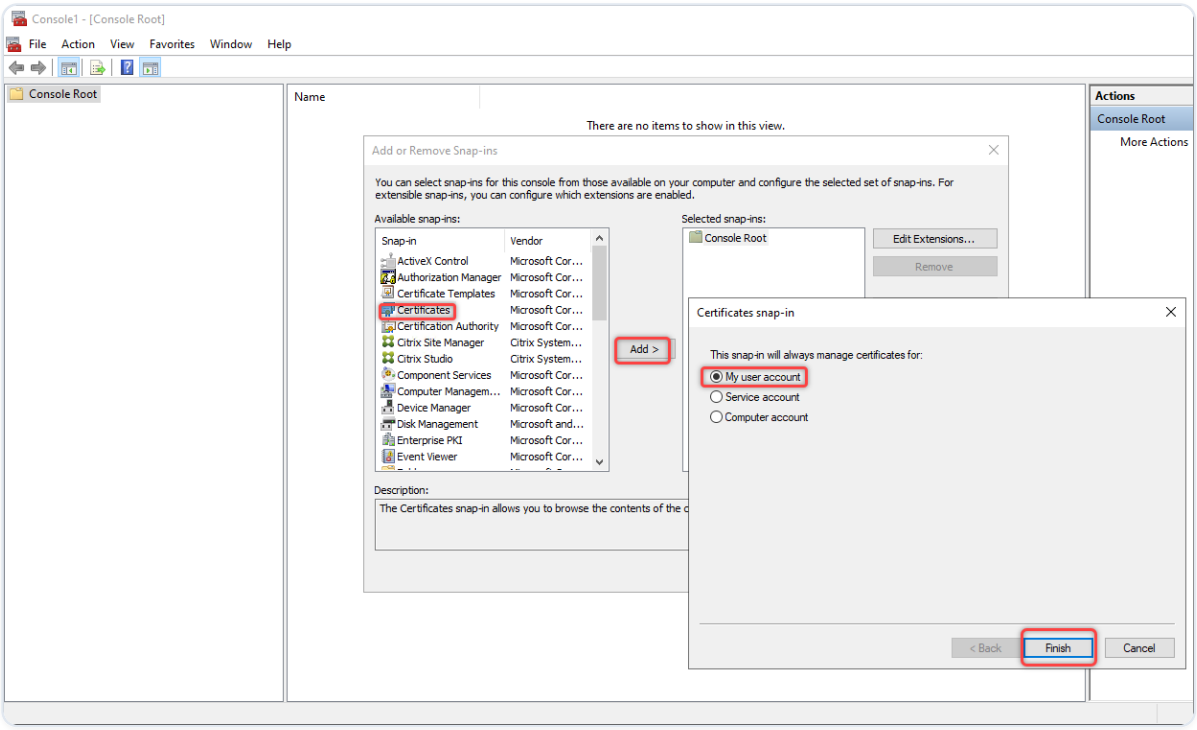
## Etapa 3: Registrar certificados para usuários de cartão inteligente

**Observação:**

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

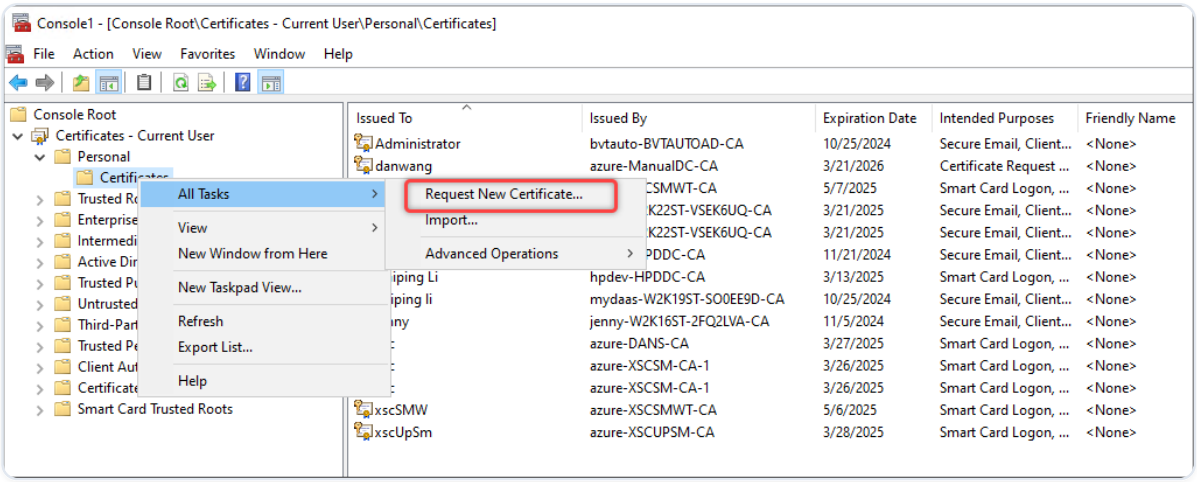
Em uma máquina Windows física ingressada no domínio, siga estas etapas para registrar certificados para cada cartão inteligente:

1. Prepare uma máquina Windows física ingressada no domínio para o uso de registro:
    a. Certifique-se de que o driver do cartão inteligente esteja instalado.
    b. Insira um cartão inteligente na máquina.
    c. Faça logon na máquina usando a conta de usuário que você deseja atribuir ao cartão inteligente.
2. Adicione o snap-in **Certificados** na máquina que você preparou na etapa 1. As etapas detalhadas são as seguintes:
    a. Abra **mmc**.
    b. Clique em **Arquivo** e depois clique em **Adicionar/Remover Snap-in**.
    c. Na janela **Adicionar ou Remover Snap-ins** que aparece, selecione **Certificados** e depois clique em **Adicionar >**.
    d. Na caixa de diálogo que aparece, selecione **Minha conta de usuário** e clique em **Concluir**.
    e. Clique em **OK**.

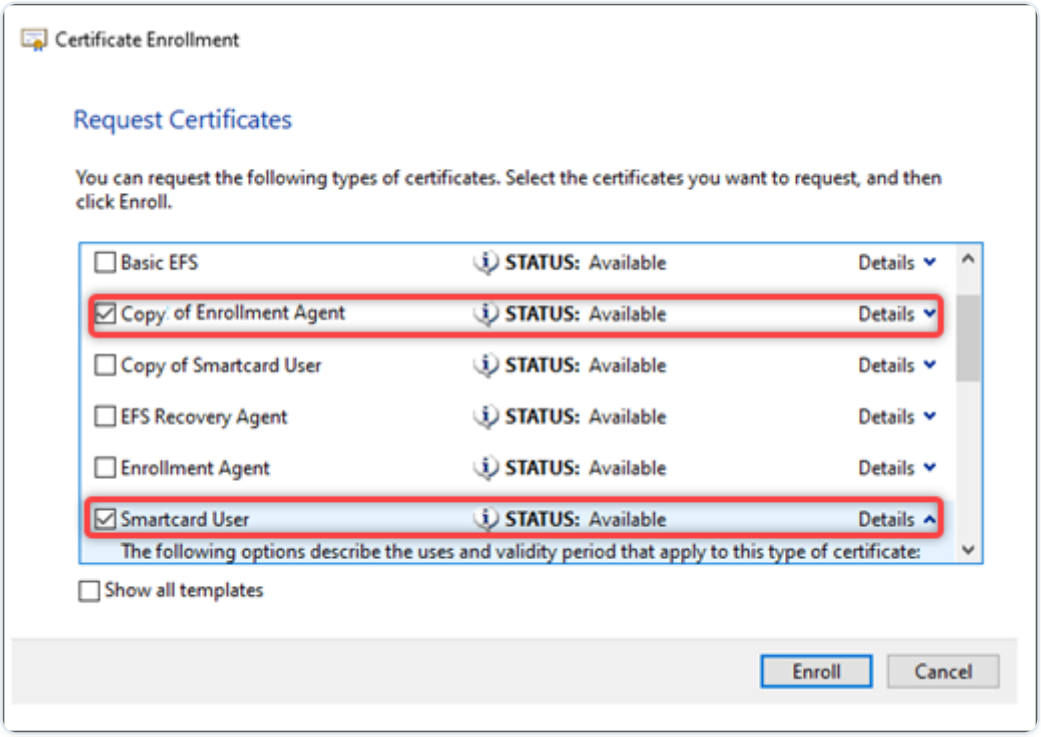



3. Solicite novos certificados para o snap-in **Certificados**. As etapas detalhadas são as seguintes:

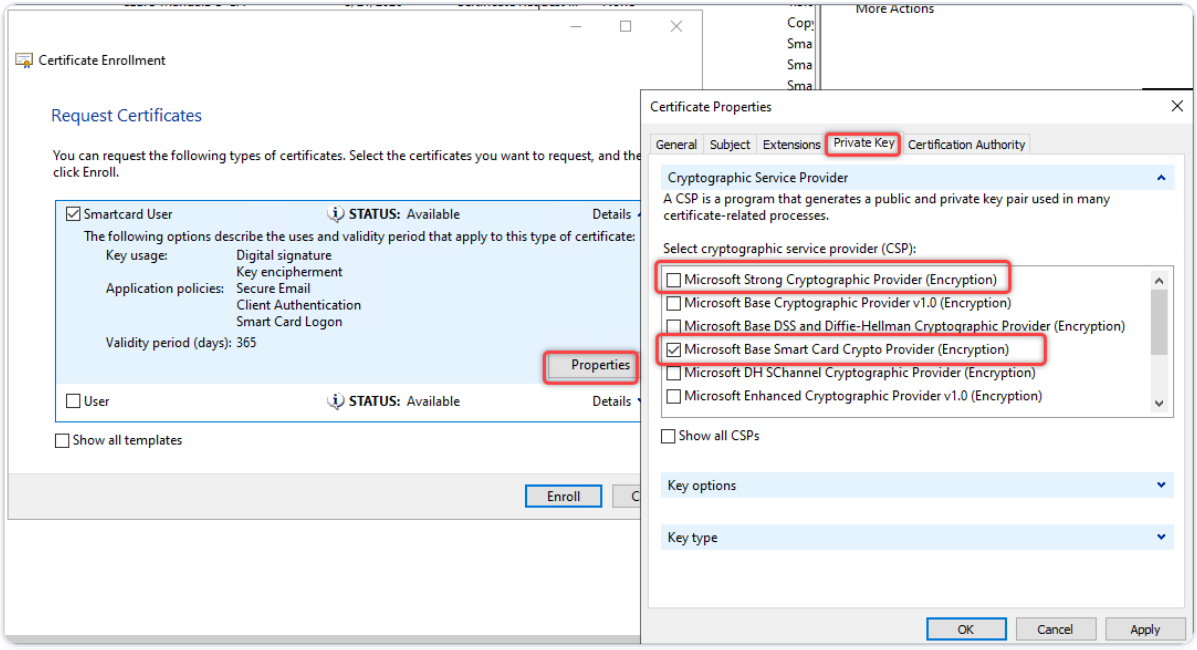
   a. Vá para **Certificados - Usuário Atual > Pessoal**, clique com o botão direito em **Certificados** e selecione **Todas as Tarefas > Solicitar Novo Certificado**.




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



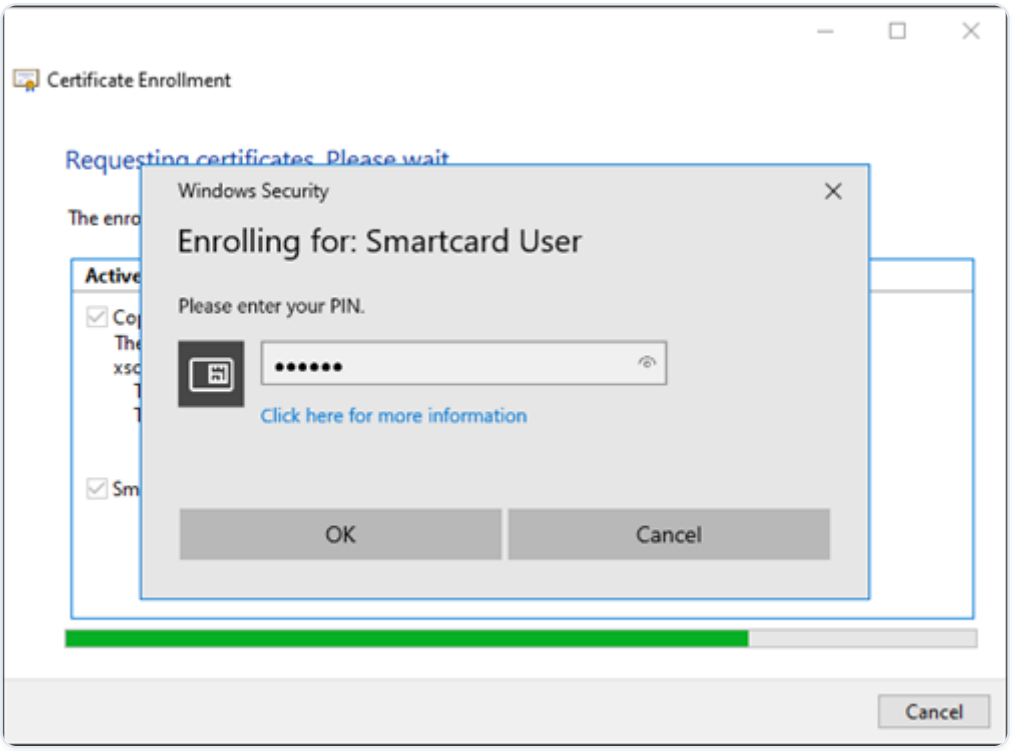

c. Na caixa de diálogo acima, clique em **Detalhes** para **Usuário de Smartcard** e depois em **Propriedades**. A caixa de diálogo **Propriedades do Certificado** aparece.



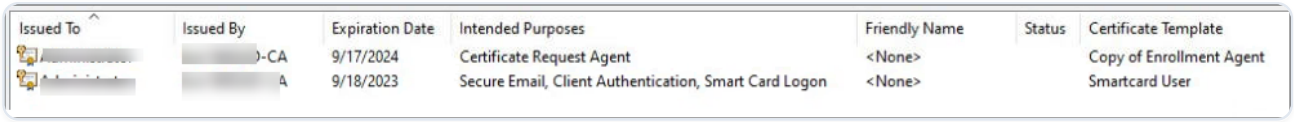

d. Na guia **Chave Privada**, expanda **Provedor de Serviços Criptográficos**, desmarque **Microsoft Strong Cryptographic Provider (Criptografia)**, selecione apenas **Microsoft Base Smart Card Crypto Provider (Criptografia)** e clique em **OK**.

e. Clique em **Registrar**.

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




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




## Etapa 4: Configurar servidores IIS do Web Studio

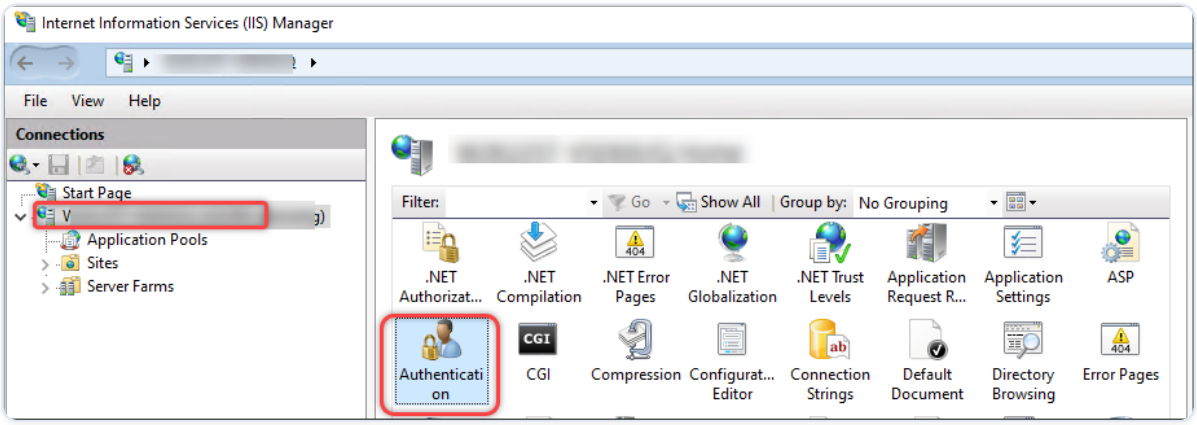
Em cada servidor Web Studio, siga estas etapas para configurar o IIS para autenticação de smart card:

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

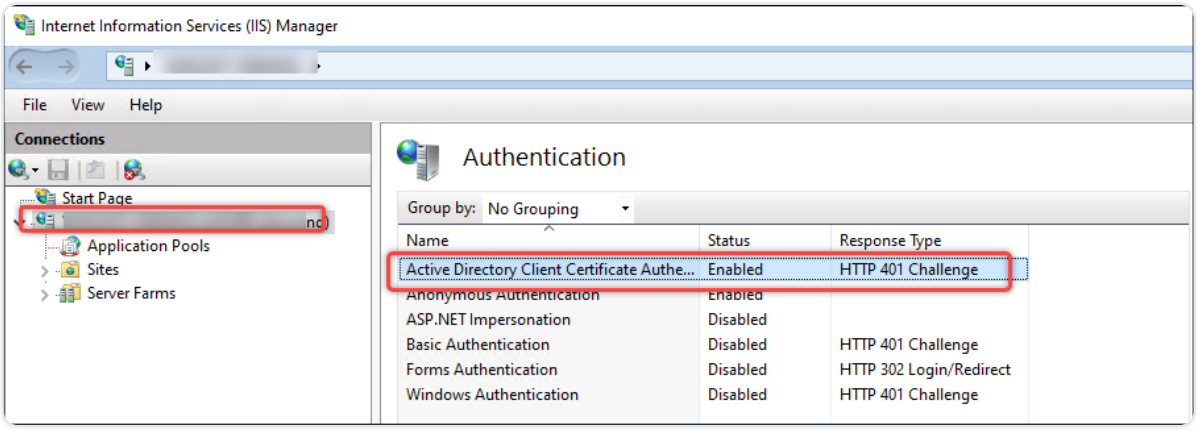
   O `<clientCertificateMappingAuthentication>` elemento está indisponível na instalação padrão do IIS 7 e posterior. Para obter mais informações sobre instalação e habilitação, consulte este artigo da Microsoft.

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

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

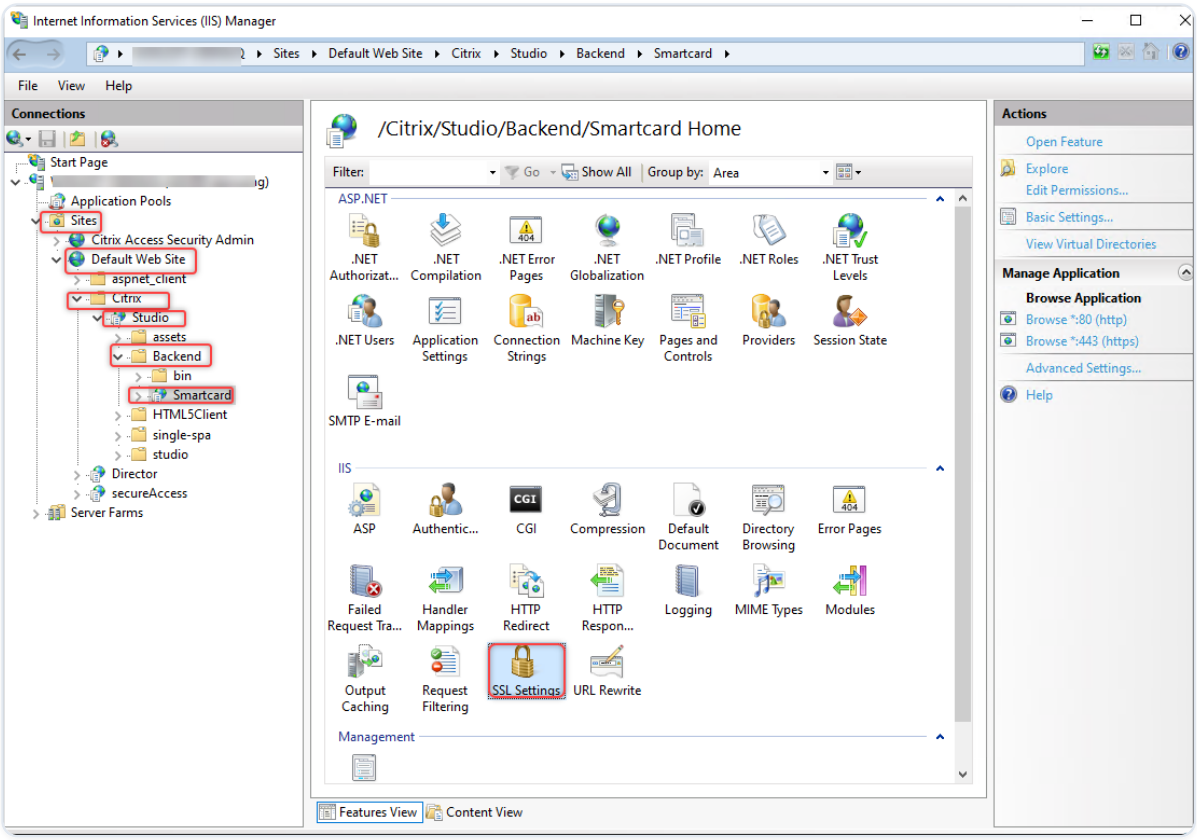



b. Habilite **Autenticação de Certificado de Cliente do Active Directory**.

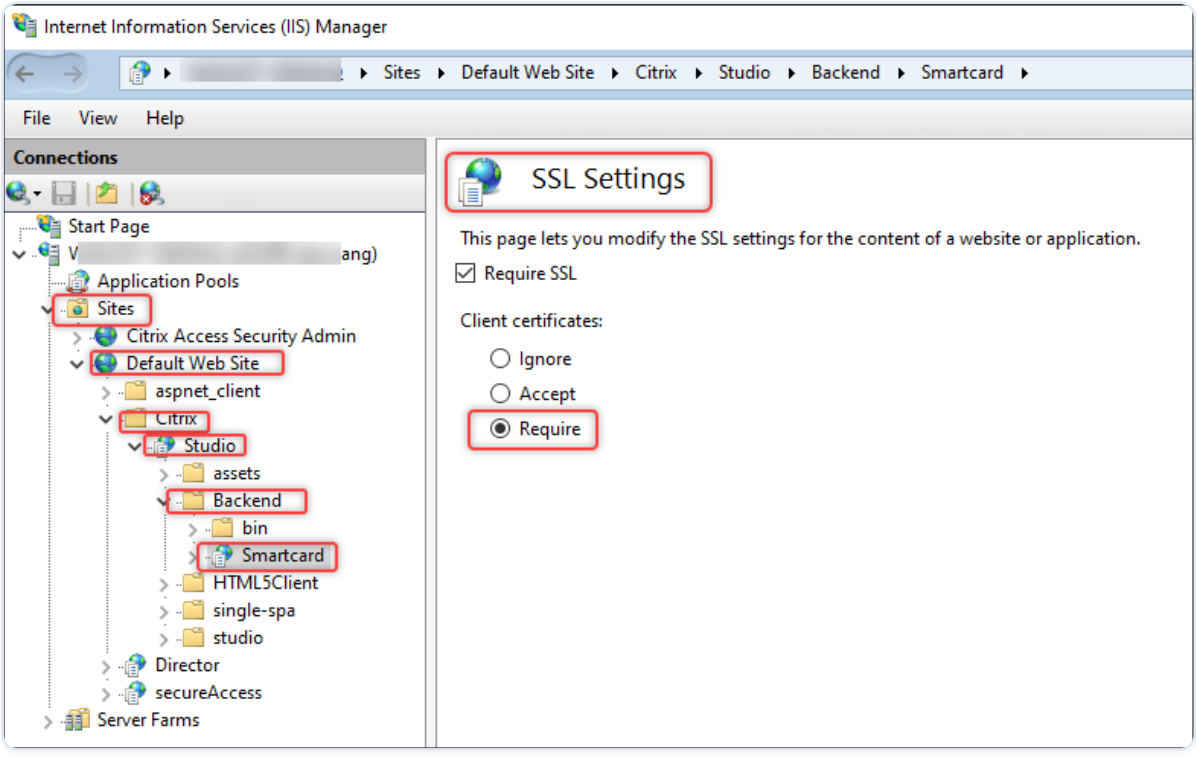



4. Configure o módulo de Back-end do Web Studio para um protocolo HTTPS mais seguro com autenticação de certificado de cliente:

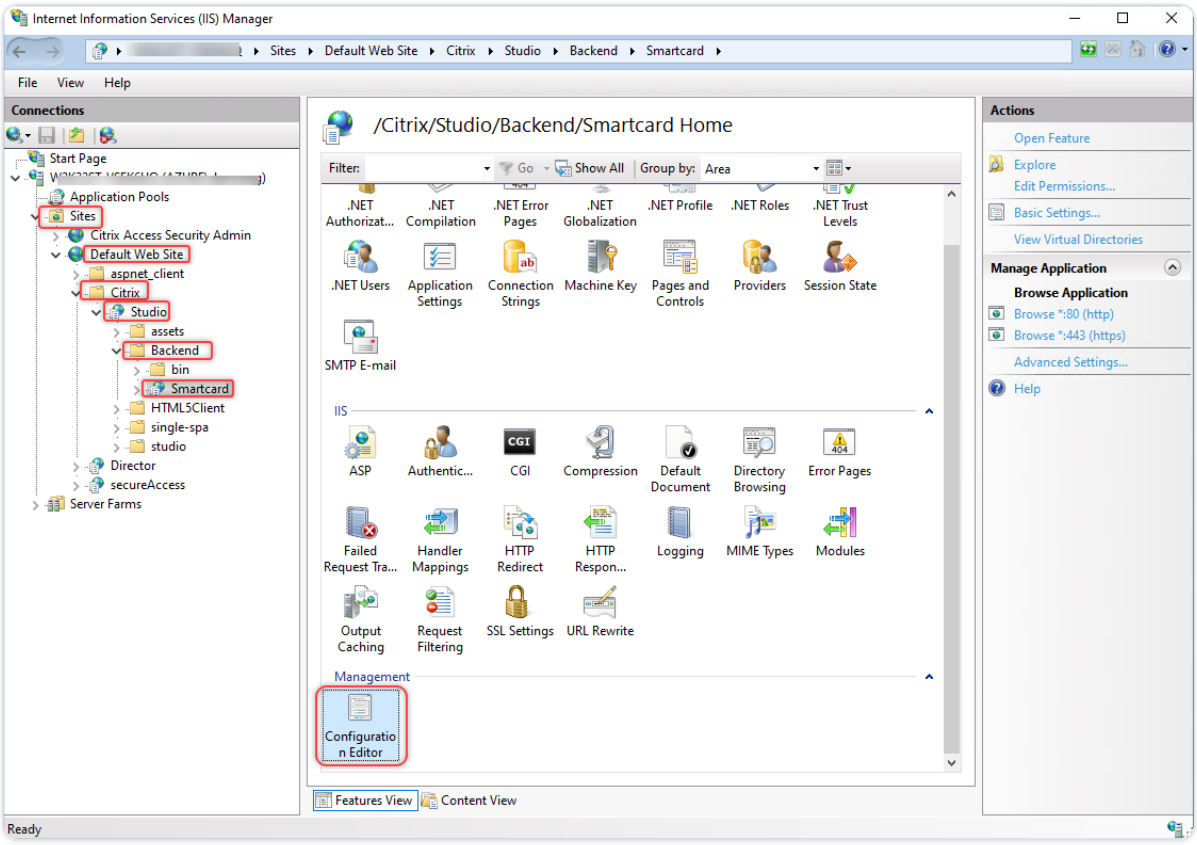
   a. Vá para **Sites > Default Web Site > Studio > Backend > Smartcard** e, em seguida, clique duas vezes em **SSL Settings** na seção **IIS**.



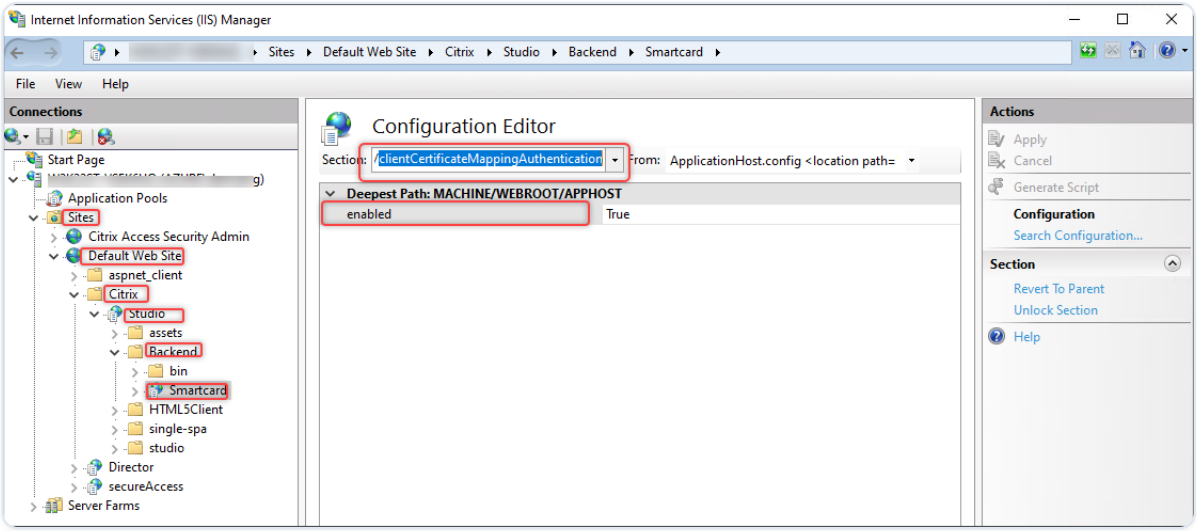

b. Selecione **Exigir** para **Certificados de cliente**.




c. Retorne a **Sites > Default Web Site > Studio > Backend > Smartcard** e, em seguida, clique duas vezes em **Configuration Editor** na seção **IIS**.




d. Certifique-se de que **/clientCertificateMappingAuthentication** esteja **habilitado**.

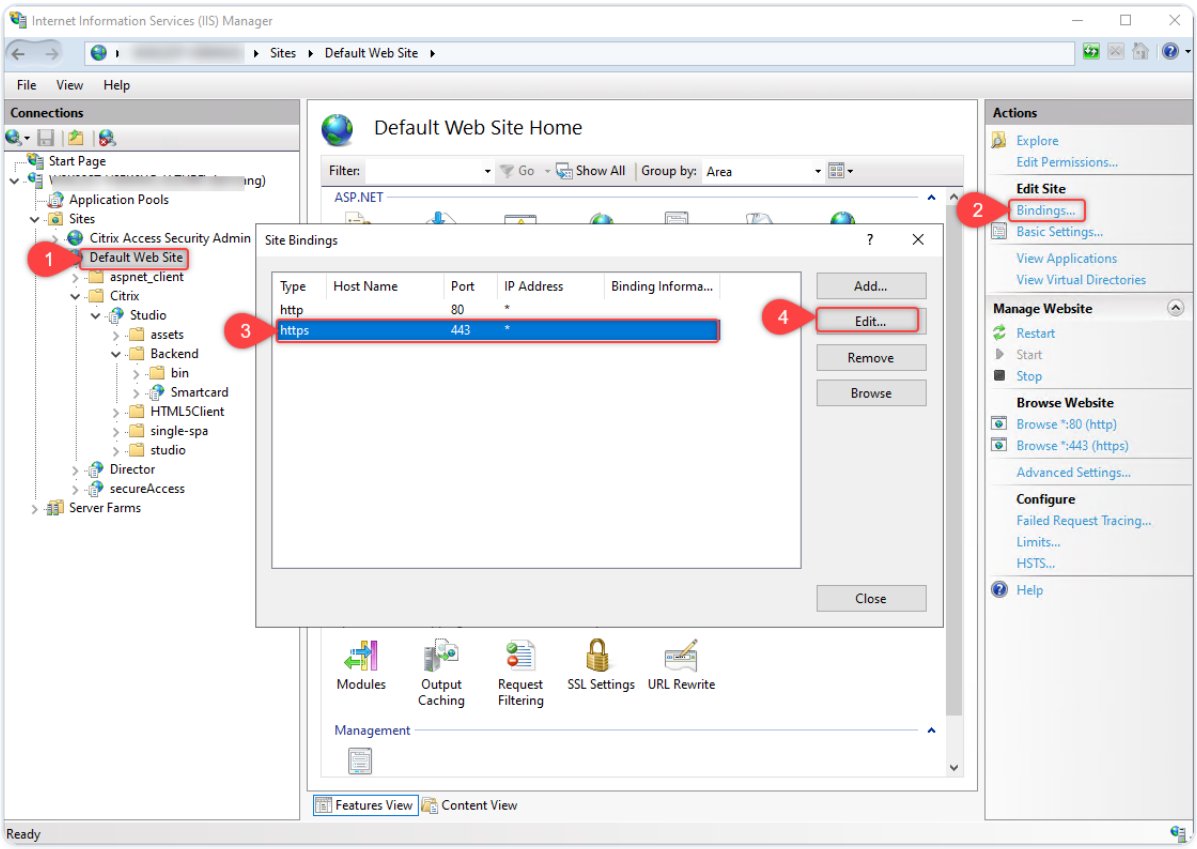



5. (Somente Windows 2022) Desabilite TLS 3.1 sobre TCP. As etapas detalhadas são as seguintes:

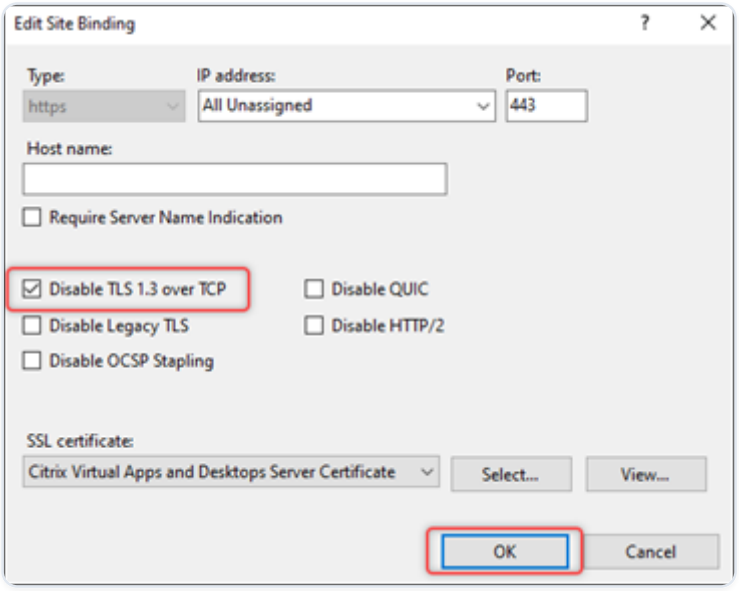
   a. Vá para **Sites > Default Web Site**.

   b. Clique em **Edit Site > Binding**.

   c. Na caixa de diálogo **Site Bindings** que aparece, selecione o registro **https** e, em seguida, clique em **Edit**.




d. Na caixa de diálogo **Edit Site Binding** que aparece, selecione **Disable TLS 1.3 over TCP** e, em seguida, clique em **OK**.




**É bom saber:**

O Web Studio Backend é um módulo no Web Studio que fornece as seguintes funções:

- Autenticação de cartão inteligente.
- Recuperação de tokens de portador FMA do serviço de Orquestração usando autenticação integrada do Windows.

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

Quando o Web Studio e os Delivery Controllers são instalados em servidores diferentes, você deve configurar delegações para cada servidor Web Studio para os Delivery Controllers para os serviços HOST e HTTPS.

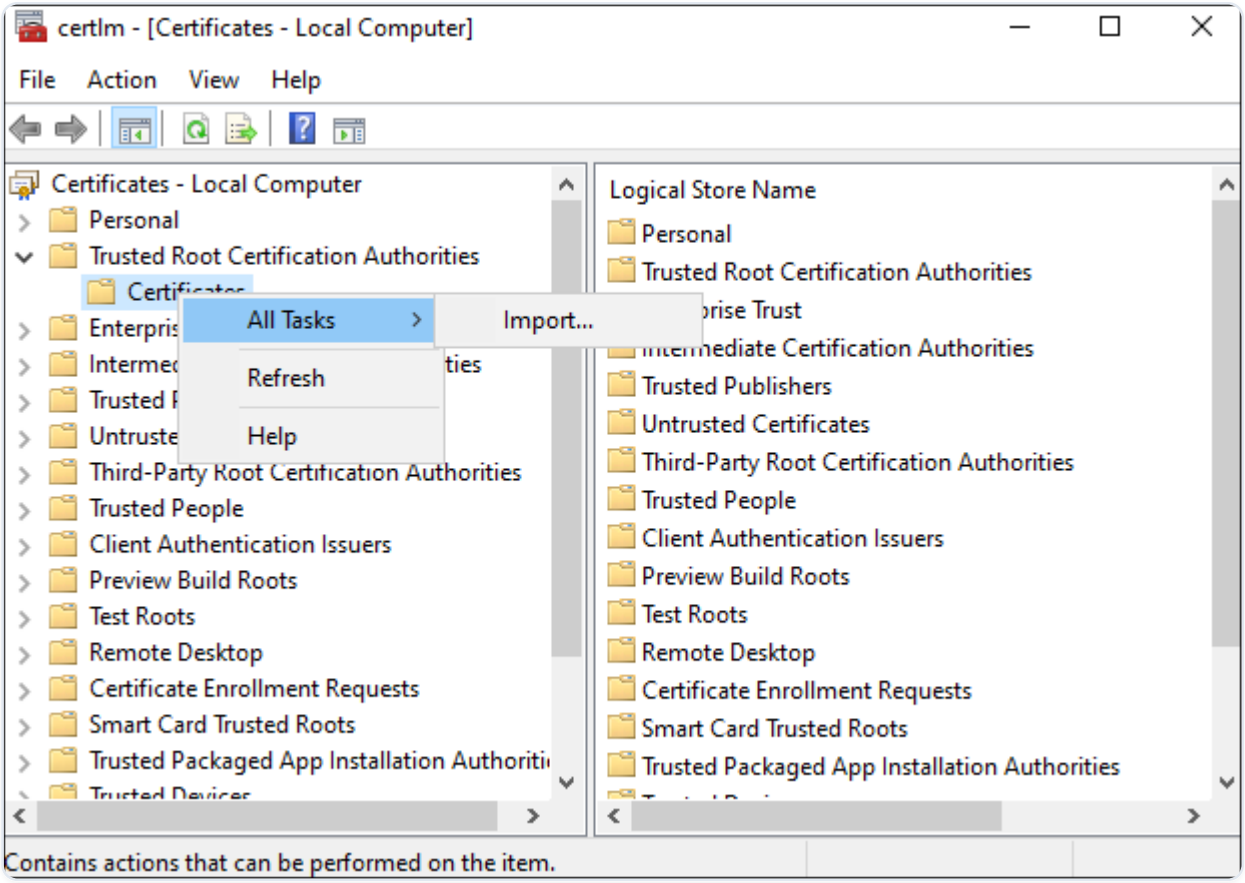
Siga estas etapas para concluir a tarefa para cada servidor Web Studio:

1. Importar o Certificado HTTPS de Orquestração do Delivery Controller™
2. Configurar delegação para o servidor Web Studio
3. Configurar delegação para a conta de serviço do servidor IIS do Web Studio

## Importar o Certificado HTTPS de Orquestração do Delivery Controller

No servidor Web Studio, importe o certificado **Delivery Controller Orchestration HTTPS** para **Autoridades de Certificação Raiz Confiáveis**. As etapas detalhadas são as seguintes:

1. Inicie **Configurações > Gerenciar certificados do computador**.
2. Clique com o botão direito do mouse em **Autoridades de Certificação Raiz Confiáveis > Certificados** e selecione **Todas as Tarefas > Importar**.

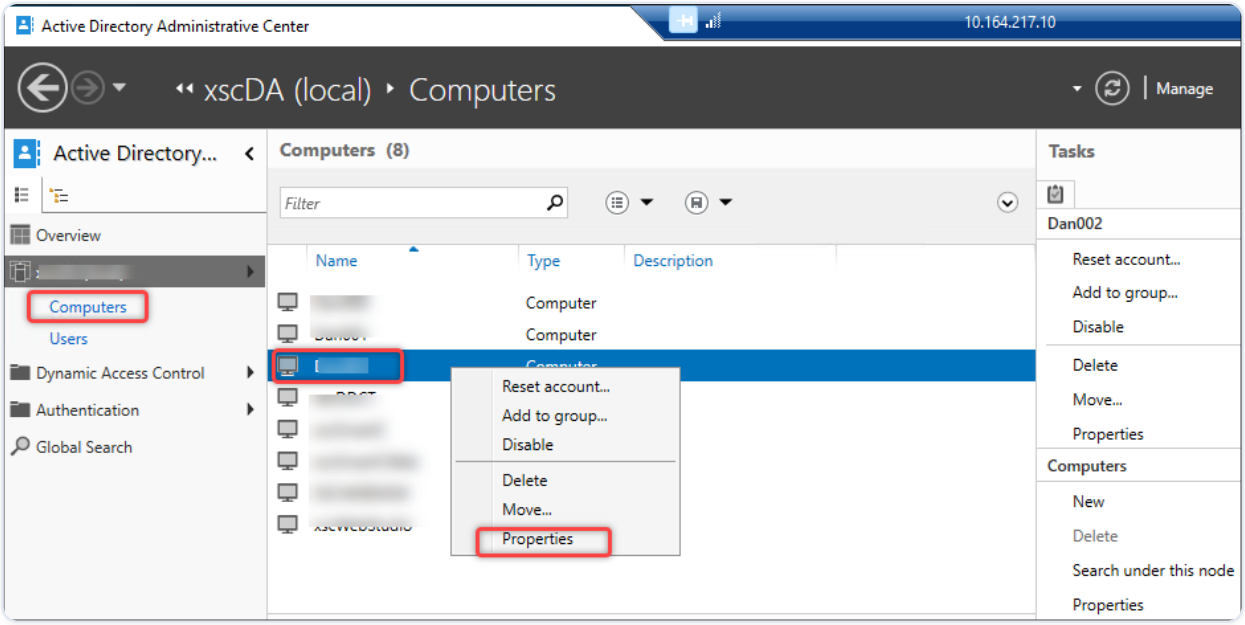


3. Siga as instruções na tela para importar o certificado **Delivery Controller Orchestration HTTPS**.

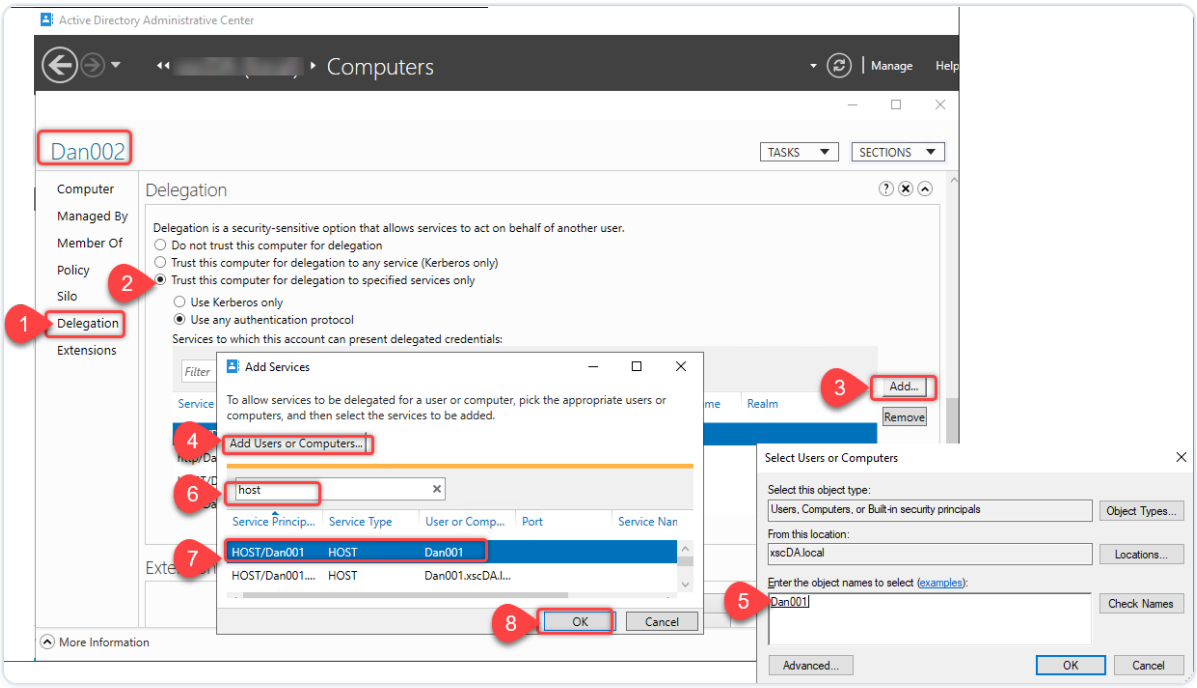
### Configurar delegação para o servidor Web Studio

No controlador de domínio, configure a delegação para o servidor Web Studio para o Delivery Controller para serviços HOST e HTTP. Siga estas etapas para concluir a tarefa:

1. No controlador de domínio, inicie o **Centro Administrativo do Active Directory**.
2. Localize a conta de **computador** do servidor Web Studio que você deseja configurar para delegação (*por exemplo, Dan002*).
3. Clique com o botão direito do mouse na conta e selecione **Propriedades**.




a. Vá para a guia **Delegação**.



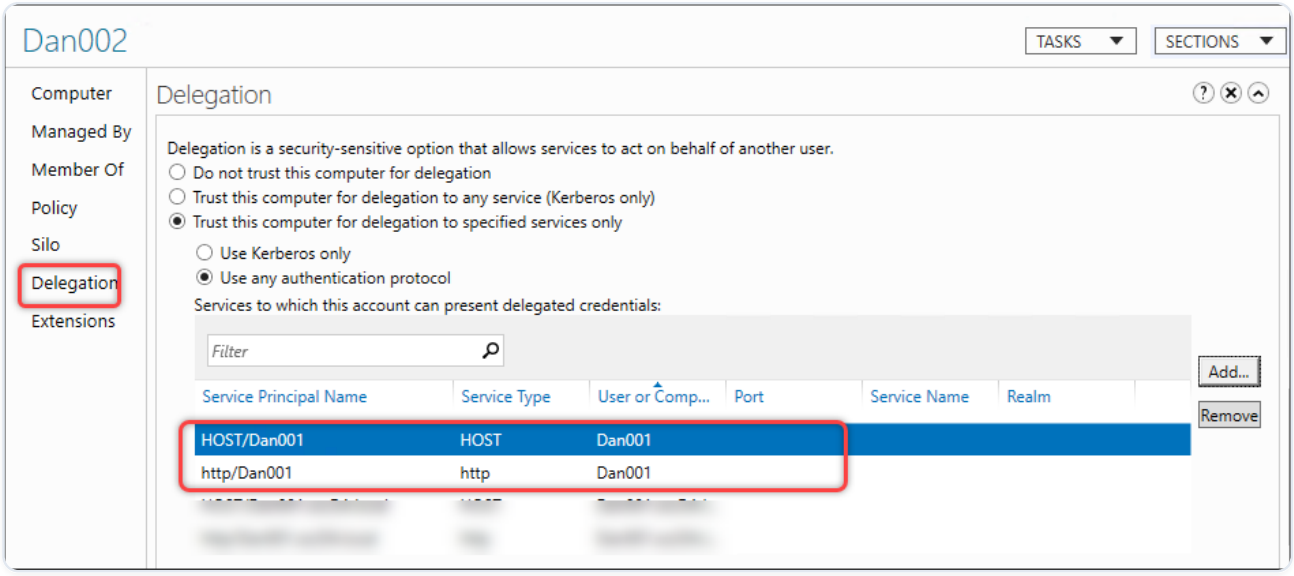

b. Selecione **Confiar neste usuário para delegação apenas a serviços especificados > Usar qualquer protocolo de autenticação**.

c. Clique em **Adicionar** para especificar a quais serviços esta conta de computador pode ser delegada.

d. Na caixa de diálogo **Adicionar Serviço** que aparece, clique em **Adicionar Usuários ou Computadores** para localizar o nome do computador do Delivery Controller (*por exemplo, Dan001*).

e. Selecione os serviços **HOST** e **HTTP** e, em seguida, clique em **OK**.

Os resultados da configuração são mostrados na captura de tela a seguir.

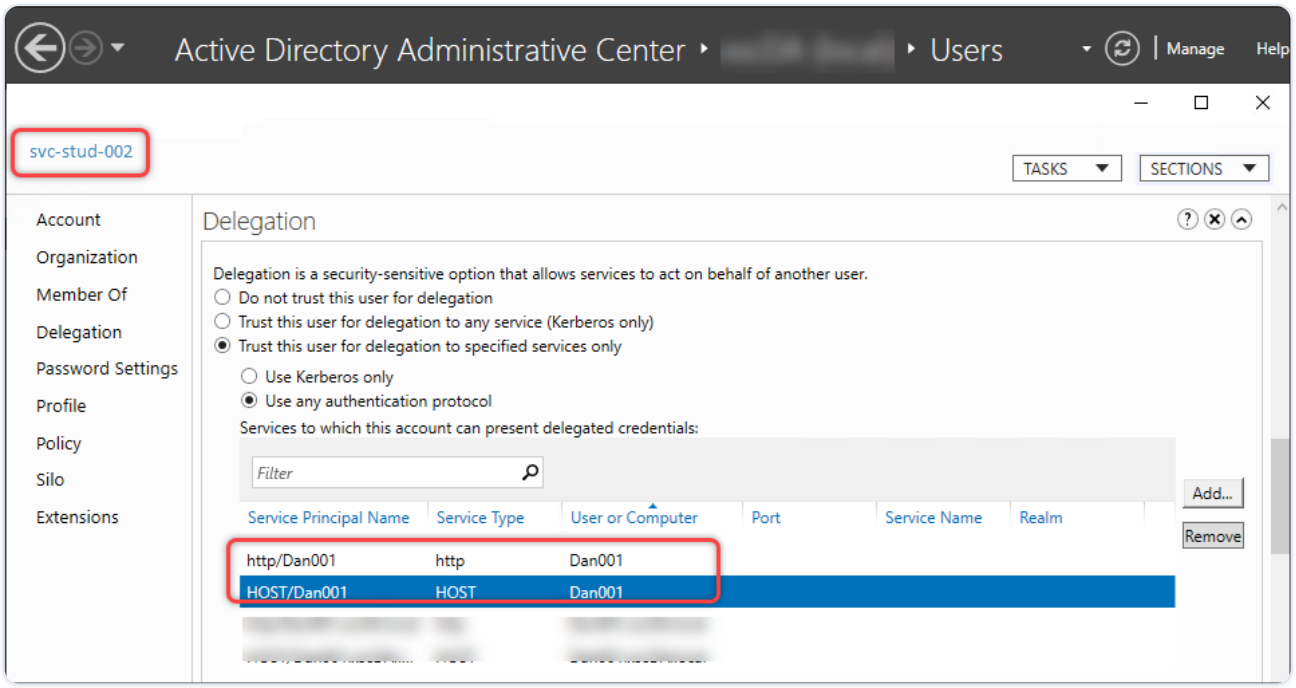


### Configurar delegação para a conta de serviço do servidor IIS do Web Studio

Se você configurou uma conta de serviço para o servidor IIS do Web Studio, também precisará configurar a delegação para esta conta de serviço para o Delivery Controller para os serviços HOST e HTTP. Com esta delegação estabelecida, o servidor Web Studio pode usar sua conta de serviço para representar o usuário atual do cartão inteligente para acessar os serviços HOST e HTTP do Delivery Group. Siga estas etapas para concluir a configuração:

1. No controlador de domínio, inicie o **Centro Administrativo do Active Directory**.
2. Localize a conta de **usuário** que você deseja configurar para delegação (*por exemplo, svr-stud-002*).
3. Clique com o botão direito do mouse na conta e selecione **Propriedades**.
4. Siga o procedimento descrito na etapa 2 para delegar a Conta de Serviço IIS do Web Studio aos serviços HOST e HTTP do Delivery Controller.

Os resultados da configuração são mostrados na captura de tela a seguir.

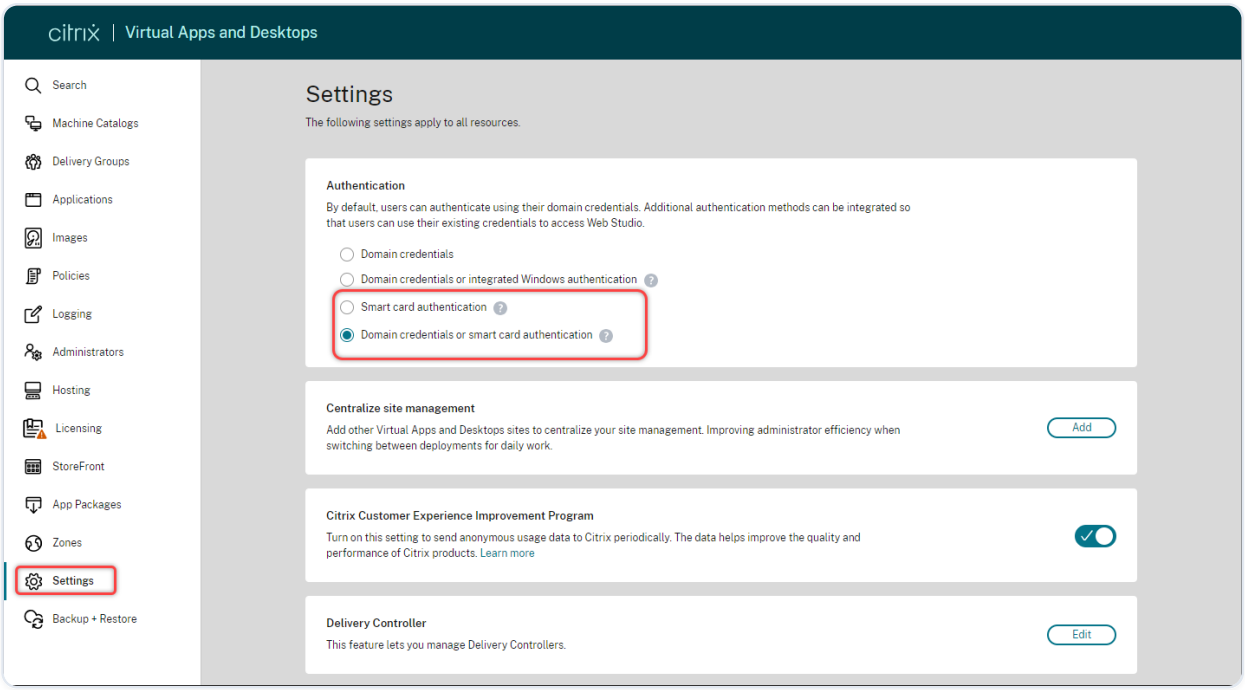



## Etapa 6: Habilitar a autenticação de cartão inteligente para o Web Studio

Siga estas etapas para habilitar a autenticação de cartão inteligente para o Web Studio:

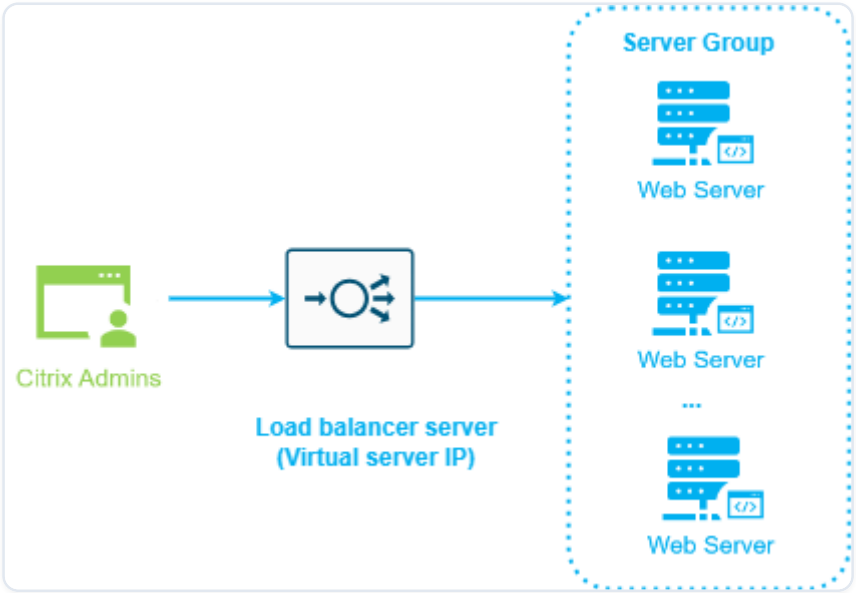
1. Faça login no **Web Studio** e selecione **Settings** no painel esquerdo.
2. Selecione **Smart card authentication** ou **Domain credentials + Smart card authentication** conforme necessário.

3. Selecione **Smart card authentication** ou **Domain credentials or smart card authentication** conforme necessário.
4. Clique em **Aplicar**.




# Configurar uma implantação do Web Studio com balanceamento de carga

Para configurar implantações do Web Studio de alta disponibilidade, você pode escolher ferramentas como NetScaler® ADC ou Balanceamento de Carga de Rede do Windows. Este artigo fornece um guia passo a passo sobre como configurar uma implantação do Web Studio com balanceamento de carga usando um dispositivo NetScaler ADC.



## Requisitos de certificado

Antes de comprar um certificado de uma autoridade de certificação comercial ou emitir um de sua autoridade de certificação corporativa, considere as seguintes opções com base nas suas necessidades:

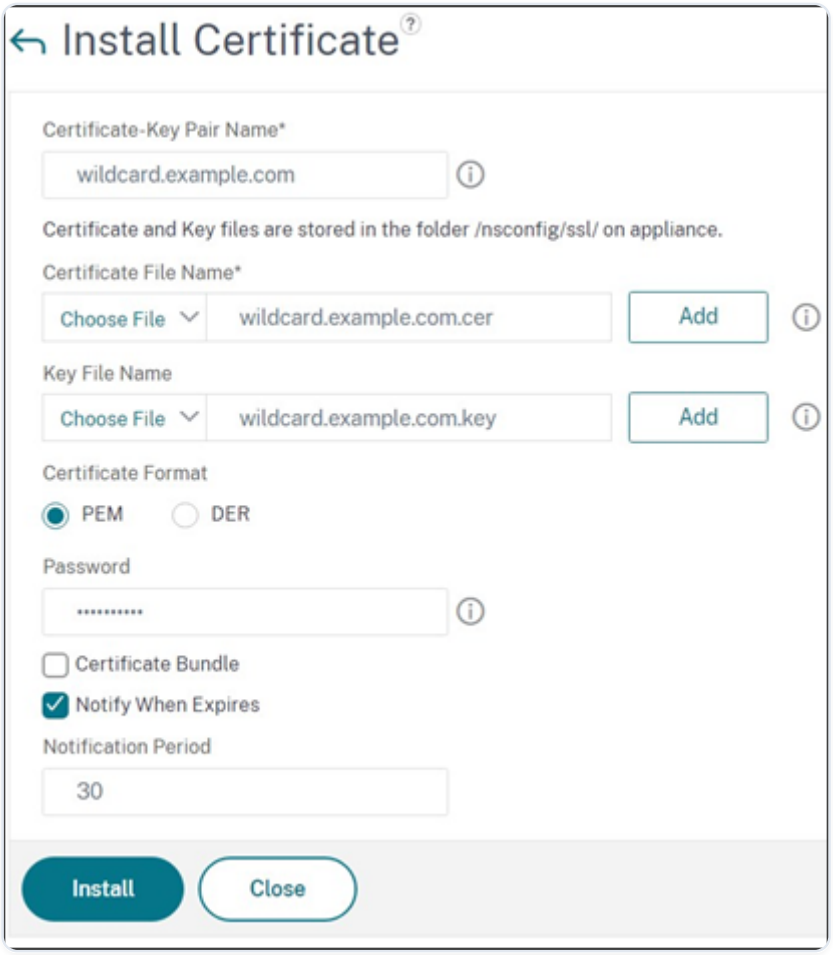
| OPÇÃO | PRÓS | CONTRAS |
| --- | --- | --- |
| Opção 1: Use um certificado curinga **.example.com* tanto no servidor de balanceamento de carga do dispositivo NetScaler ADC quanto nos servidores Web Studio. | • Simplifica a configuração<br>• Mais fácil de gerenciar (certificado único)<br>• Pode adicionar novos subdomínios sem atualizar o certificado | • Se o certificado curinga for comprometido, todos os subdomínios estarão em risco<br>• Nem todos os aplicativos suportam certificados curinga<br>• Pode ser mais caro do que certificados individuais |
| Opção 2: Use um certificado com Nomes Alternativos de Assunto (SANs) tanto no servidor de balanceamento de carga do dispositivo NetScaler ADC quanto nos servidores Web Studio. | • Flexível, pode incluir vários domínios e subdomínios específicos | • O gerenciamento de entradas SAN pode se tornar complexo à medida que o número de domínios aumenta |

| OPÇÃO | PRÓS | CONTRAS |
|---|---|---|
| | Centraliza o gerenciamento para vários domínios | Adicionar novos domínios requer a reemissão do certificado |
| | Suporta vários nomes distintos, oferecendo mais flexibilidade do que curingas | Limitado pelo número de entradas SAN suportadas pela CA |
| Opção 3: Usar um certificado para cada servidor Web Studio e para o servidor balanceador de carga do dispositivo NetScaler ADC | • Cada servidor é protegido independentemente | • Maior sobrecarga administrativa, pois cada certificado deve ser gerenciado separadamente |
| | A violação de um certificado não afeta os outros | Mais certificados para renovar e custos potencialmente mais altos |
| | Pode usar certificados específicos adaptados às necessidades de cada servidor | Deve garantir que todos os certificados estejam configurados de forma consistente |

### Configurar o certificado do servidor no balanceador de carga

1. Faça logon na GUI de gerenciamento do dispositivo NetScaler ADC.
2. Selecione **Gerenciamento de Tráfego > SSL > Certificados > Certificados de Servidor**
3. Clique em **Instalar**.

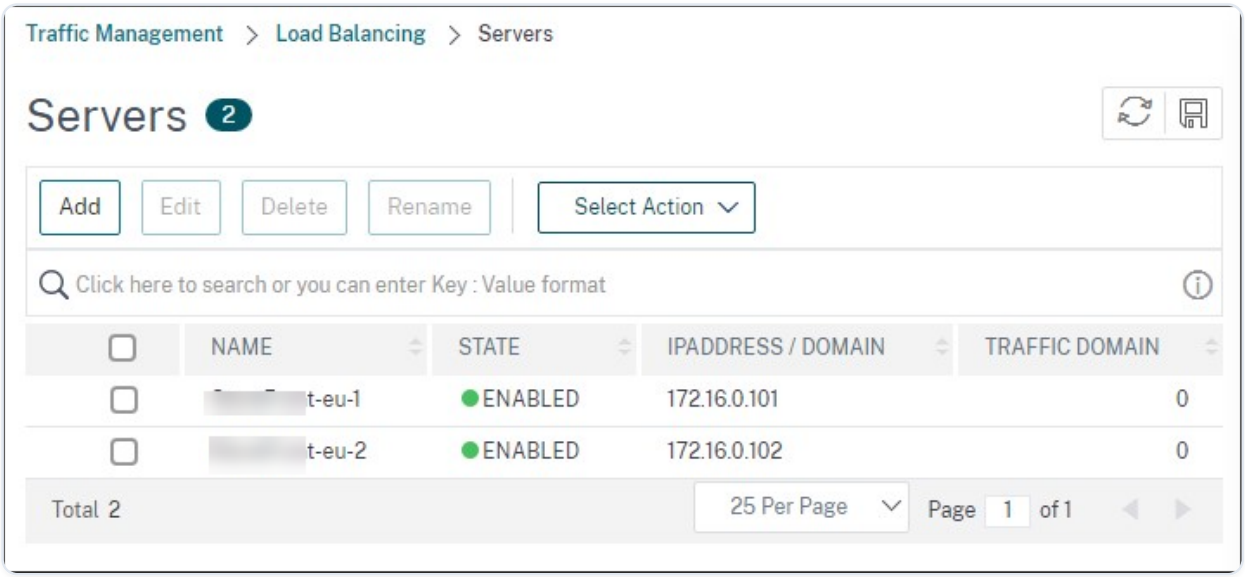
4. Na página **Instalar Certificado de Servidor**, insira um Nome de Par de Chaves de Certificado, clique em **Escolher Arquivo** e então procure o arquivo de certificado. Se o arquivo de certificado não incluir a chave privada, selecione um **Arquivo de Chave**.




## Etapa 1: Adicionar nós de servidor do Web Studio

Adicione todos os nós de servidor do Web Studio (por exemplo, `Studio-eu-1` e `Studio-eu-2`) ao balanceador de carga.

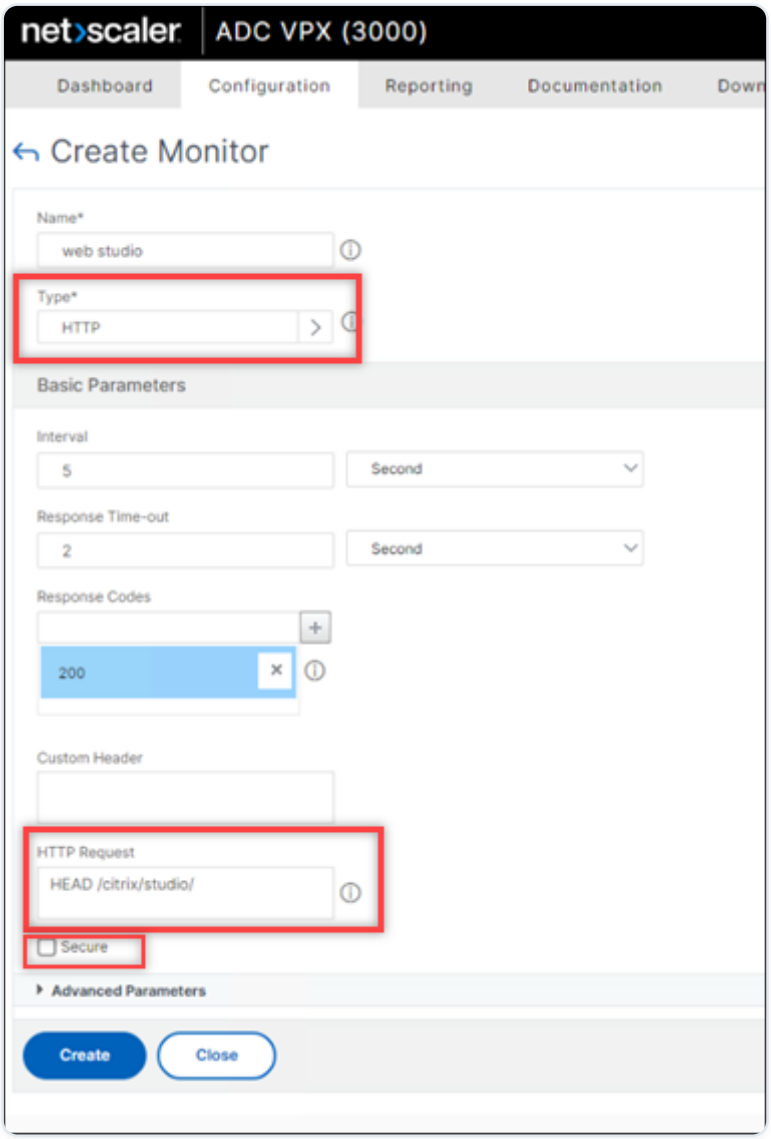
1. Faça logon na GUI de gerenciamento do NetScaler ADC.
2. navegar para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**. Clique em **Adicionar**.
3. Insira o endereço IP do servidor de um nó de servidor do Web Studio.
4. Repita as etapas 2–3 para adicionar os outros servidores do Web Studio.




## Etapa 2: Adicionar um monitor para nós de servidor do Web Studio

Configure um monitor no balanceador de carga para verificar o status de todos os nós de servidor do Web Studio.

1. Selecione **Gerenciamento de Tráfego > Balanceamento de Carga > Monitores > Adicionar**.
2. Na guia **Configuração**, conclua as seguintes configurações e deixe os outros padrões:
   - Insira **Web Studio** para **Nome**.
   - Selecione **HTTP** ou **SSL** para **Tipo**.
   - Selecione a opção **Seguro**.
   - Insira **HEAD/citrix/studio/** para **Solicitação HTTP**.



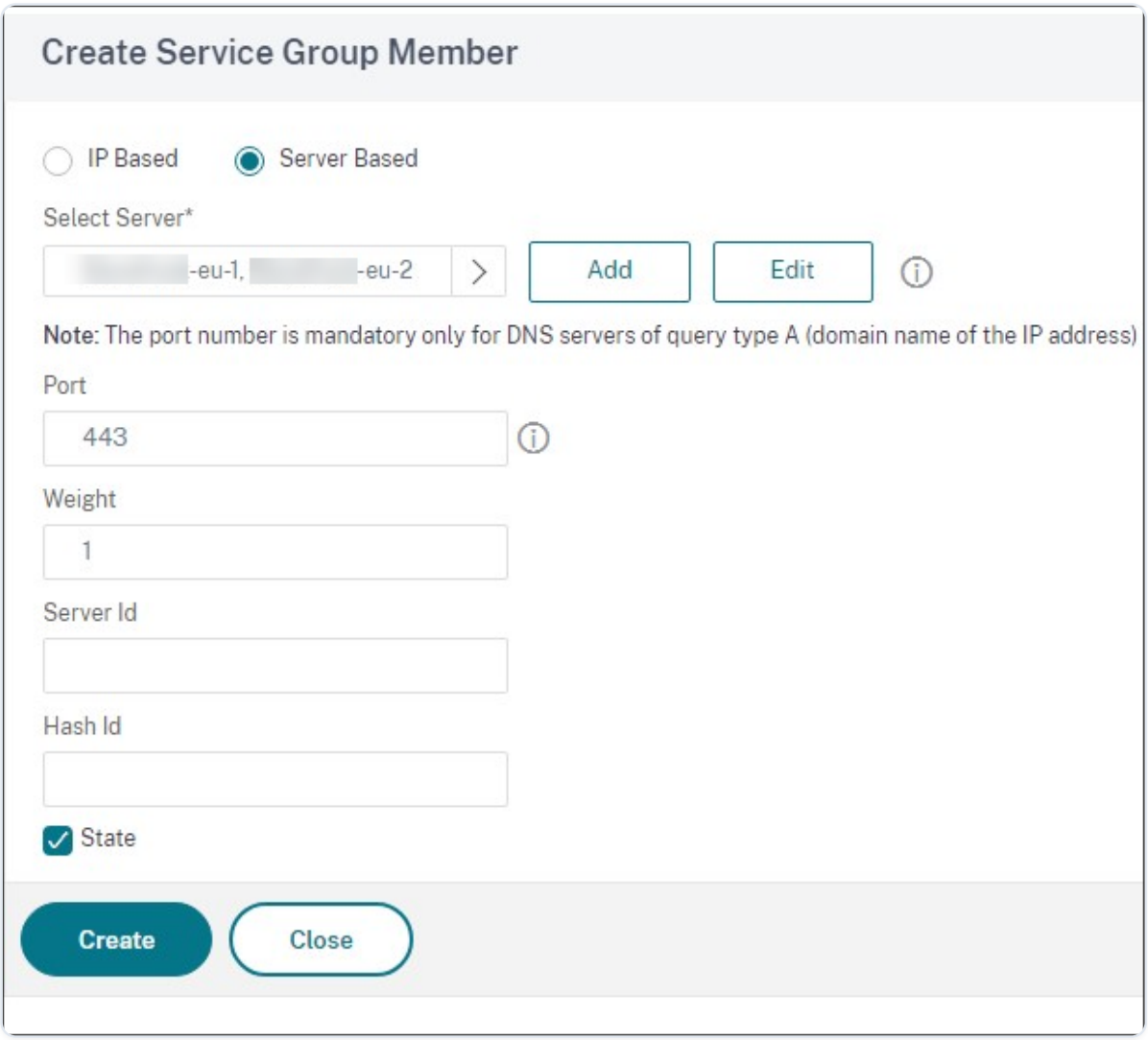

## Etapa 3: Crie um grupo de serviços para nós de servidor do Web Studio

1. Selecione **Gerenciamento de Tráfego > Balanceamento de Carga > Grupos de Serviços > Adicionar**. Para se conectar aos servidores do Web Studio via HTTPS, selecione um protocolo SSL, deixe as outras configurações como padrão e clique em **OK**.
2. Dentro do seu Grupo de Serviços, em **Membros do Grupo de Serviços**, clique em **Nenhum Membro do Grupo de Serviços** e siga estas etapas para adicionar membros:

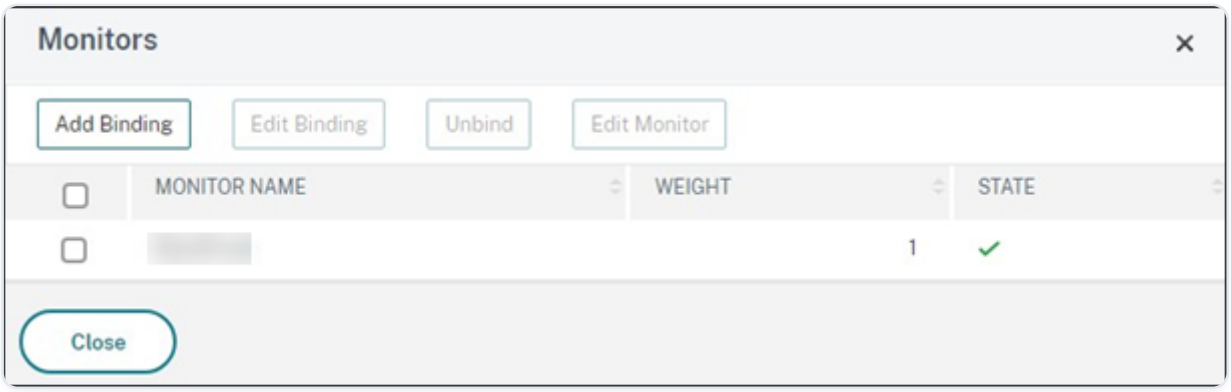
    a. Clique em **Baseado em Serviço**.

    b. Selecione todos os servidores que você adicionou anteriormente.

    c. Insira **443** para a porta.



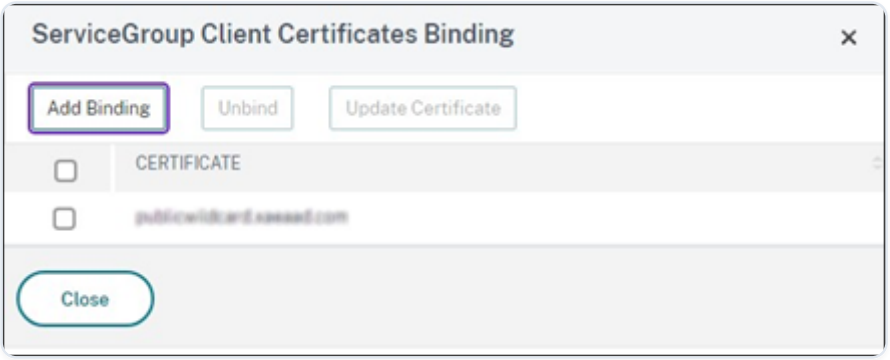

3. Adicione a seção **Monitores** e selecione o monitor do Web Studio que você criou anteriormente.




4. Adicione a seção **Certificados** e conclua as seguintes configurações:

   a. Vincular o certificado do cliente.

   b. Vincule o certificado da CA usado para assinar o certificado do servidor que você importou anteriormente e quaisquer outras CAs que possam fazer parte da cadeia de confiança PKI.




5. Adicione a seção **Configurações**, selecione **Inserir Cabeçalho IP do Cliente** e, em seguida, insira um nome de cabeçalho de **X-Forwarded-For**. Essa configuração permite que o Endereço IP do Cliente seja usado em Políticas.

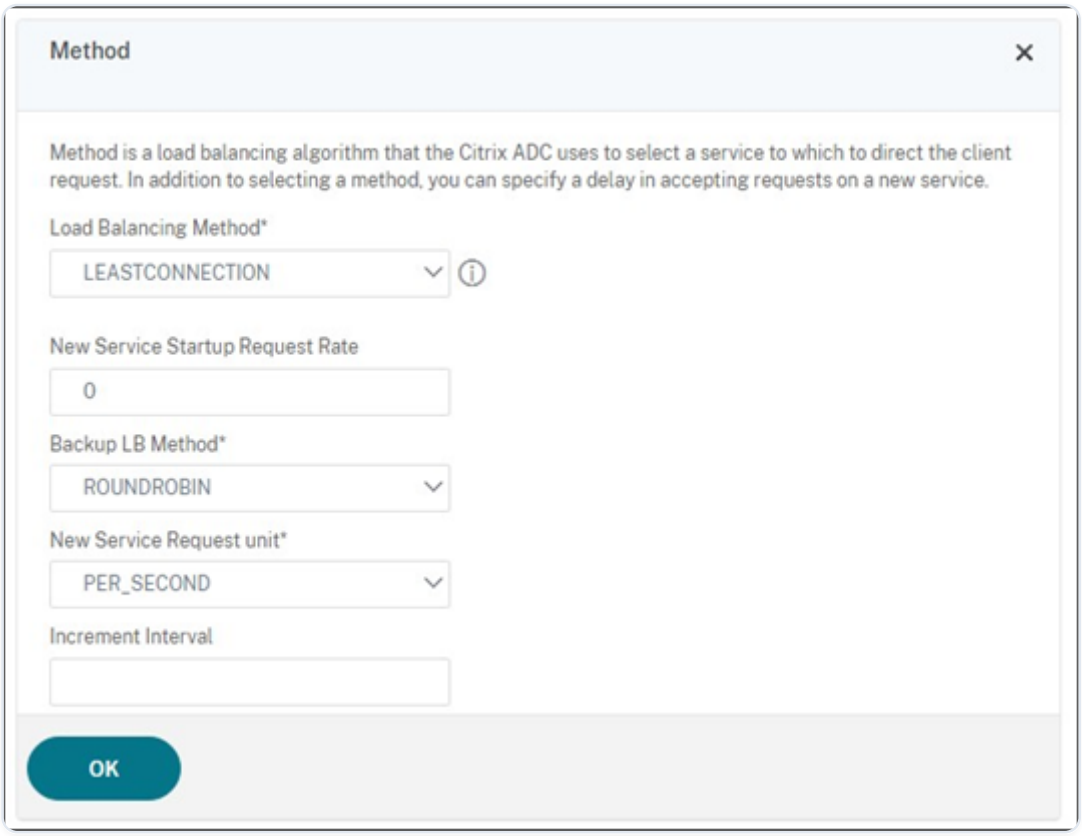
## Etapa 4: Criar um servidor virtual

Crie um servidor virtual de balanceador de carga para que os usuários acessem o grupo de servidores do Web Studio.

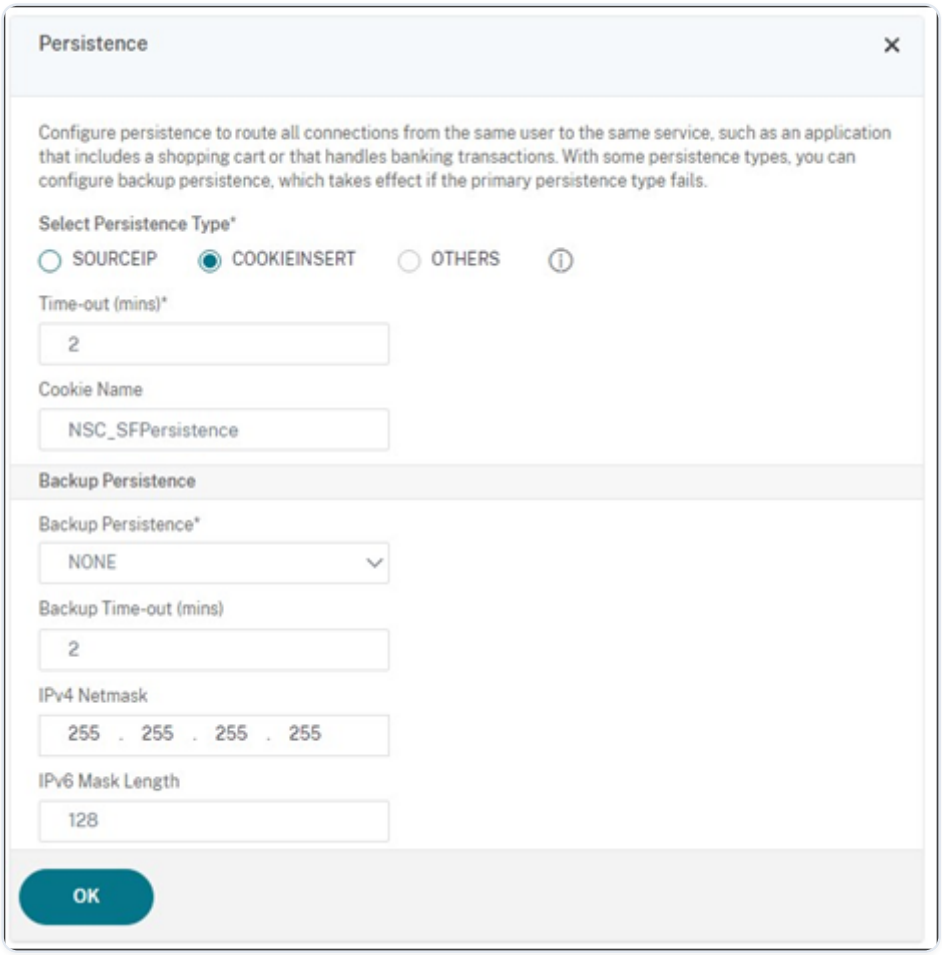
1. navegar até **Traffic Management > Load Balancing > Virtual Servers** e, em seguida, clique em **Add**.
2. Insira um nome, selecione **SSL** para o **Protocolo**, insira **443** para a **Porta** e, em seguida, clique em **OK**.



3. Vincule o **Grupo de Serviço** que você criou anteriormente ao servidor virtual de balanceamento de carga.
4. Vincule o certificado da CA que você vinculou ao grupo de serviço em Etapa 3: Criar um grupo de serviço para nós de servidor do Web Studio.
5. Adicione a seção **Método** e selecione o método de balanceamento de carga. As opções comuns para balanceamento de carga do Web Studio são **ROUNDROBIN** ou **LEASTCONNECTION**.




6. Adicione a seção **Persistência** e conclua as seguintes configurações:
   a. Defina o método de persistência como **COOKIEINSERT**.
   b. Defina o tempo limite para ser o mesmo que o tempo limite da sessão no Web Studio (por padrão, 20 minutos).
   c. Nomeie o cookie para facilitar a depuração futura. Por exemplo, **NSC_SFPersistence**.
   d. Defina a persistência de backup como **NENHUM**.




**Observação:**

Se o cliente não tiver permissão para armazenar o cookie HTTP, as solicitações subsequentes não terão o cookie HTTP, e a Persistência não será usada.

## Etapa 5: Crie registros DNS para o servidor virtual

No Controlador de Domínio, crie um registro DNS e PTR para mapear o endereço IP do servidor virtual para um FQDN. Os usuários do Web Studio em sua rede usam este FQDN para acessar o grupo de servidores do Web Studio. Por exemplo, webstudio.example.com resolve para o endereço IP do servidor virtual do balanceador de carga (VIP).

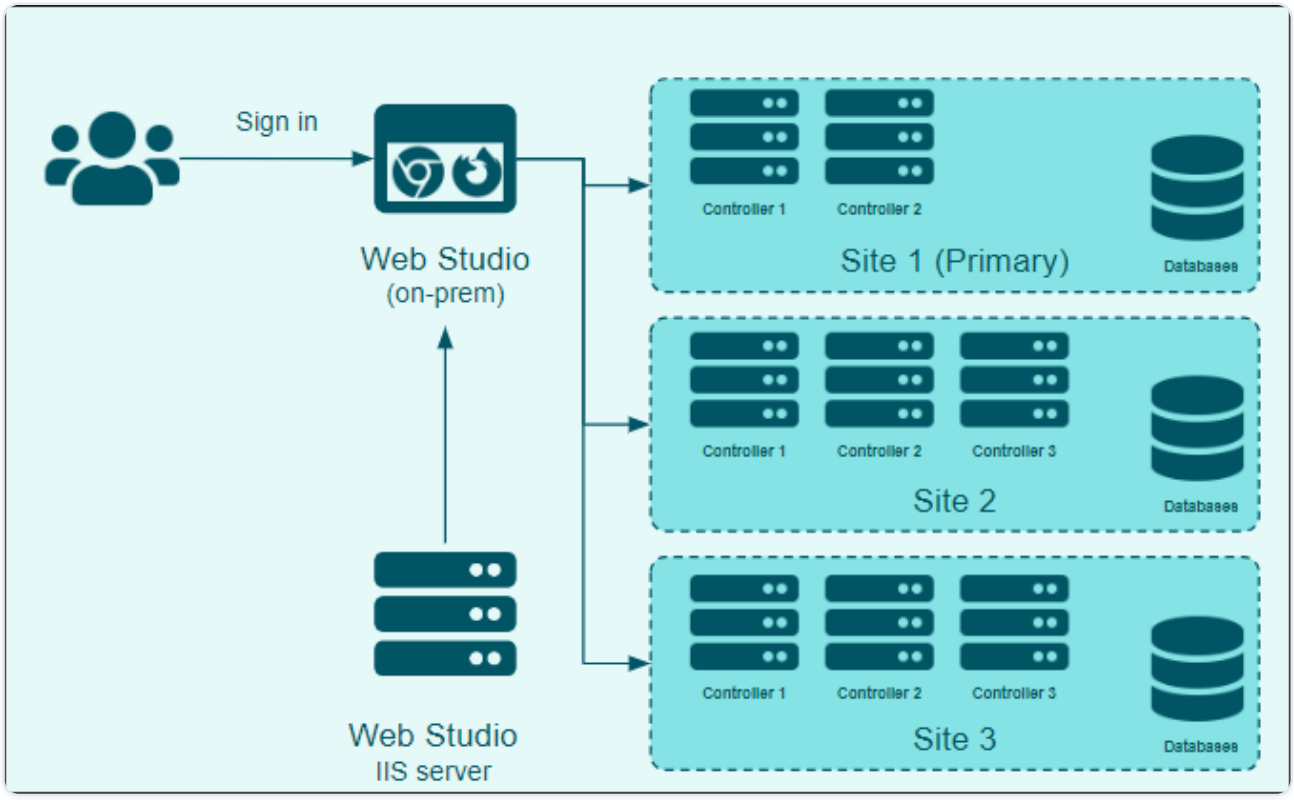
Captura de tela da seção de persistência(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/new-dns.png)

Forneça esta URL para os usuários acessarem os servidores do Web Studio: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`. Exemplo: `https://webstudio.example.com/citrix/studio`

# Habilitar gerenciamento de vários sites

Por padrão, um console do Web Studio é mapeado para um único site do Citrix Virtual Apps and Desktops™, e, quando necessário, você pode configurar um console do Web Studio para gerenciar vários sites. Dessa forma, você pode ter apenas um Web Studio instalado para configurar e gerenciar todos os seus sites.

O diagrama a seguir ilustra a arquitetura de múltiplos sites, onde uma única implantação do Web Studio gerencia múltiplos sites independentes do Citrix Virtual Apps and Desktops.




## Benefícios

- Melhora a eficiência ao gerenciar múltiplos sites com uma experiência unificada de logon único.
- Facilita a solução de problemas com todas as configurações acessíveis a partir de um único console.

## Considerações

Ao configurar e implantar os sites, tenha em mente os seguintes itens:

- Versão necessária:
  - Citrix Virtual Apps and Desktops 2311 e posterior.

- A versão do Delivery Controller™ deve corresponder à versão do Web Studio ou ser anterior a ela, com um requisito mínimo de 2311 ou posterior.
- Este recurso é exclusivo do Web Studio (baseado na web) e não está disponível no Citrix Studio (baseado em Windows).

- Para oferecer suporte ao logon único, implante todos os sites em domínios confiáveis.
- Você pode gerenciar um máximo de 10 sites do Citrix Virtual Apps and Desktops usando o console unificado do Web Studio.

## Fluxo de trabalho

### Antes de começar

- Determine o site principal e certifique-se de que o console do Web Studio esteja acessível para o gerenciamento do site principal.

  **Observação:**

  - Ao projetar um site primário, esteja ciente de que a acessibilidade dos sites adicionados depende da disponibilidade do site primário. Problemas de desempenho com o site primário podem afetar o acesso aos sites adicionados.
  - Se o Web Studio não estiver instalado, consulte Instalar o Web Studio.

- Certifique-se de que os sites que você pretende gerenciar com o Web Studio já estejam configurados.
  - Para criar um novo site, consulte Criar um site.
- (Recomendado) Para habilitar o logon único ao alternar entre os sites no console, habilite a Autenticação Integrada do Windows (IWA) em todos os sites. Para os sites onde o IWA não está habilitado, você também pode usar suas credenciais de logon para fazer login.

### Etapa 1: Faça login no console do Web Studio

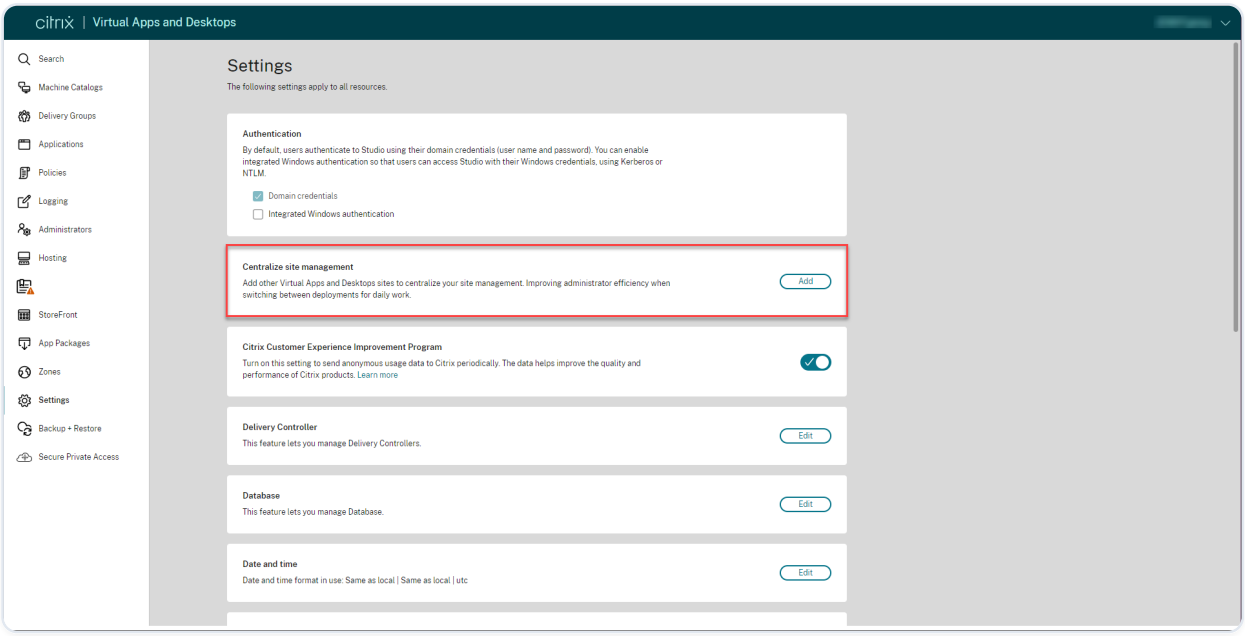
1. Abra um navegador da web. Digite `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Faça login no Web Studio para gerenciar o site primário.

**Observação:**

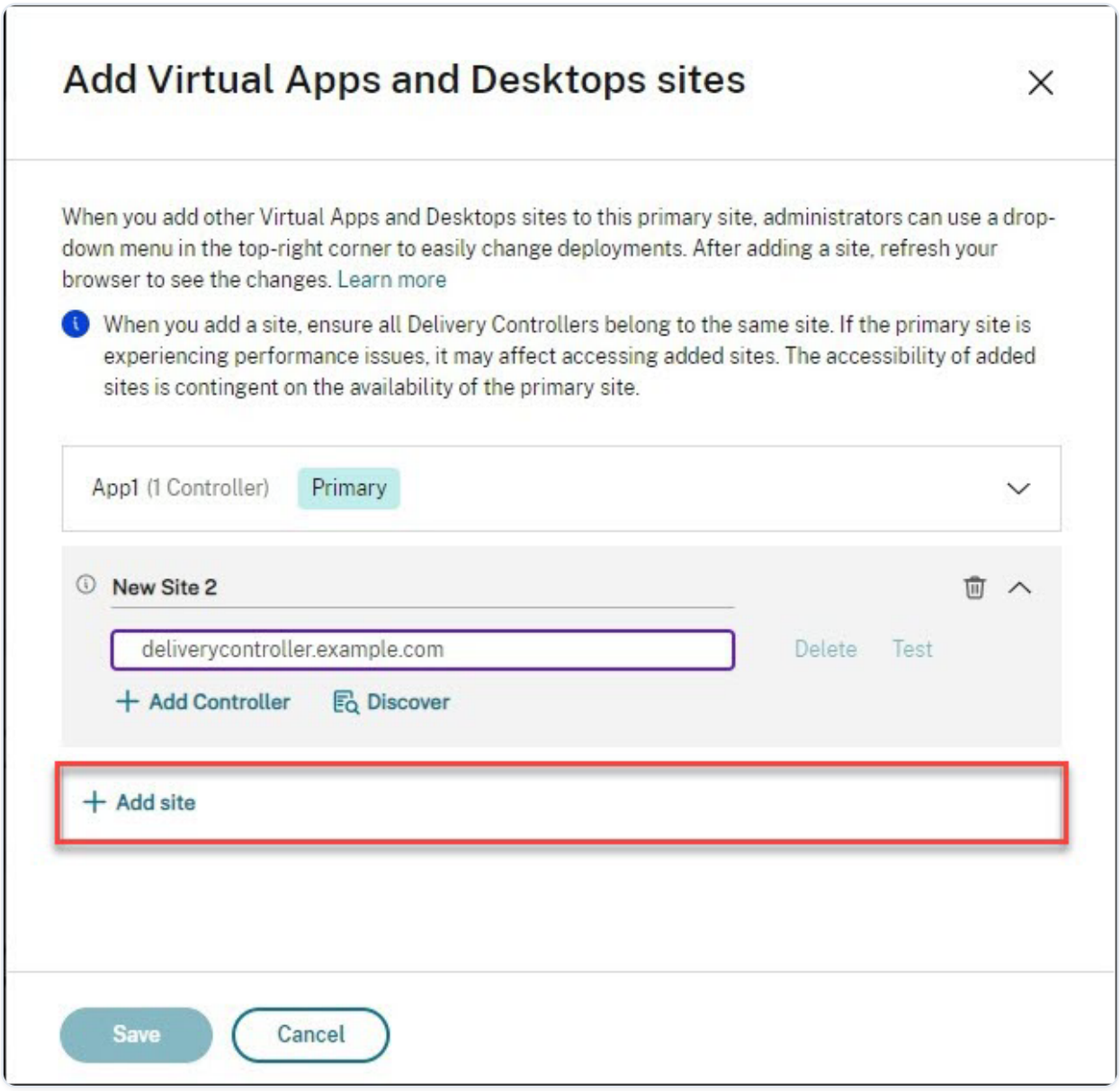
O endereço do Delivery Controller que você usa durante a instalação identifica o site. Se o Delivery Controller for do site primário, você fará login nesse site.

## Etapa 2: Adicionar sites usando o Web Studio

1. Vá para **Configurações** > **Gerenciamento centralizado de sites** e clique em **Adicionar**.




2. Na página **Adicionar sites do Virtual Apps and Desktops**, clique em **Adicionar site**.



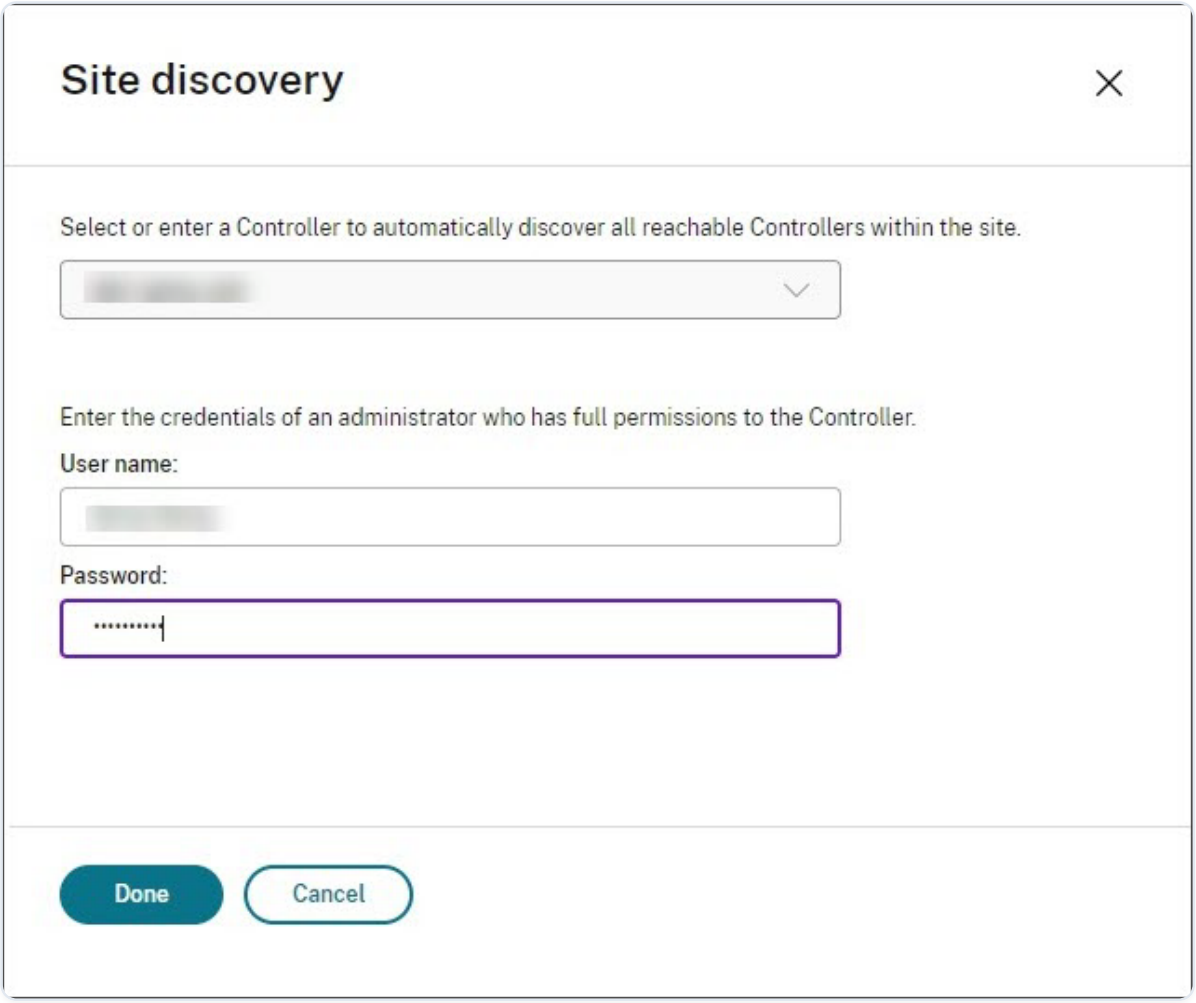

3. Execute uma das seguintes ações para adicionar os Delivery Controllers:

   - Clique em **Adicionar Controlador** e, em seguida, insira o FQDN. Clique em **Testar** para testar sua conectividade.
   - Clique em **Descobrir**.

     a. Na página **Descoberta do site**, selecione ou insira o endereço de um Controlador presente no site.

     b. Insira as credenciais de um administrador que tenha permissão total para o Controlador nos campos **Nome de usuário** e **Senha**.

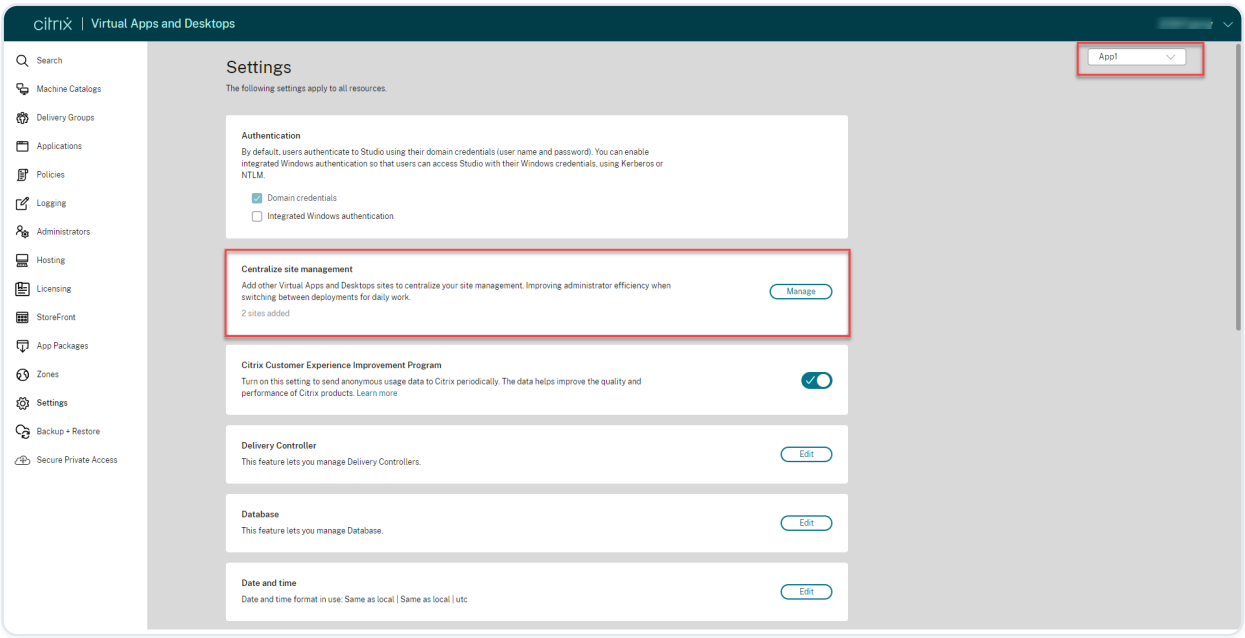
     c. clique em **Concluído**.




> **Observação:**
>
> O recurso Descobrir adiciona automaticamente os controladores de entrega acessíveis no site com base no endereço do controlador de entrega que você insere.

4. Clique em **Salvar**.

   Para gerenciar ou editar as configurações do site, vá para **Configurações** > **Gerenciamento centralizado do site** e clique em **Gerenciar**. A opção **Gerenciar** é habilitada apenas para o site principal.




### Etapa 3: Gerenciar configurações do site

Atualize seu navegador para que as alterações de configuração do site apareçam. A caixa de seleção do site aparece no canto superior direito do console.

Na página **Configurações**, selecione o site no menu suspenso no canto direito, ao lado do ícone **Atualizar**. O console exibe a configuração do site selecionado.

**Observação:**

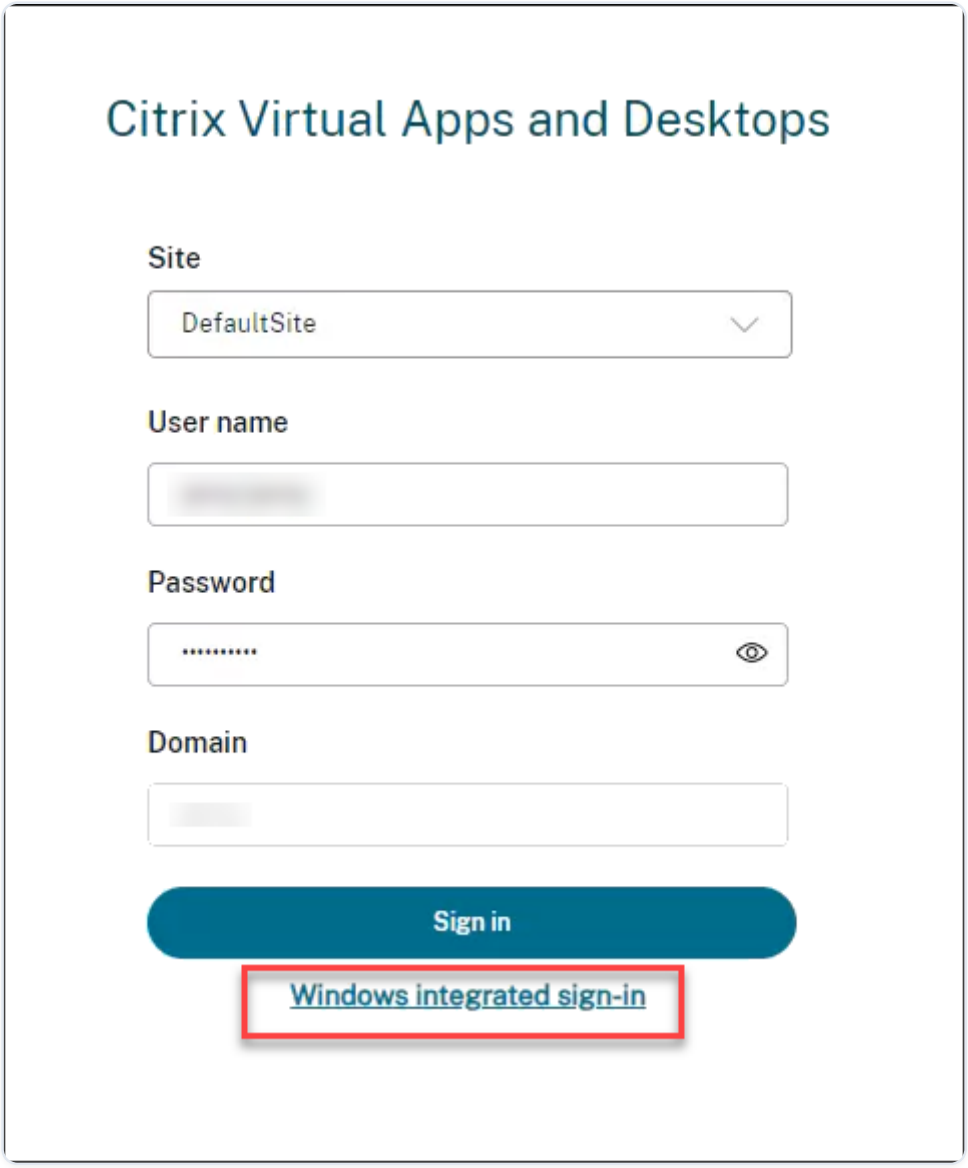
- Quando o site principal não está acessível, você não pode acessar outros sites associados a ele.
- Ao alternar para outro site, certifique-se de ter as permissões ou credenciais de acesso necessárias para fazer login.

## Experiência de login após a configuração do site

1. Abra um navegador da web. Digite `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Selecione um site no campo **Site**.
3. Selecione **Logon Integrado do Windows** ou insira o **Nome de usuário** e a **Senha** para fazer logon.

**Observação:**

O Logon Integrado do Windows está disponível apenas se estiver habilitado para o site selecionado. Para obter mais informações sobre a autenticação integrada do Windows, consulte Gerenciar autenticação.




# Identidades de máquina

Cada máquina deve ter uma identidade de máquina exclusiva, também conhecida como conta de computador. As identidades de máquina podem ser criadas e gerenciadas nas máquinas localmente ou em um diretório, como o Active Directory (AD) local ou o Azure AD. O Citrix® oferece suporte à hospedagem de aplicativos e desktops virtuais em máquinas que são

ingressadas no Active Directory, ingressadas no Azure Active Directory, ingressadas no Hybrid Azure Active Directory ou não ingressadas no domínio.

## Tipos de identidade de máquina

Os seguintes tipos de identidade de máquina são suportados.

| TIPO DE IDENTIDADE DE MÁQUINA | DESCRIÇÃO |
|---|---|
| Ingressado no AD | As identidades são criadas e gerenciadas no Active Directory local. As máquinas provisionadas são ingressadas no Active Directory local usando as identidades de máquina atribuídas. |
| Ingressado no Azure AD Híbrido | As identidades são criadas no Active Directory local e são sincronizadas com o Azure AD por meio do Azure AD Connect. As máquinas provisionadas são ingressadas no Active Directory local. As máquinas são então ingressadas no Azure AD Híbrido. Para importar uma VM ingressada no Azure AD Híbrido, a VM é tratada como uma VM ingressada no Active Directory pelo Citrix Virtual Apps and Desktops. |
| Não ingressado no domínio | As identidades são criadas e gerenciadas nas máquinas localmente. A importação de VMs para o Citrix Virtual Apps and Desktops não é suportada. |

## Configurações Suportadas

A seguir estão os detalhes das configurações suportadas para cada cenário.

## Infraestrutura suportada

| IDENTIDADE DA MÁQUINA | CITRIX APLICATIVOS VIRTUAIS E DESKTOPS™ | CITRIX WORKSPACE™ | CITRIX STOREFRONT | CITRIX GATEWAY SERVICE | CITRIX GATEWAY |
|---|---|---|---|---|---|
| Ingressado no AD | Sim | Sim | Sim | Sim | Sim |
| Ingressado no Azure AD | Não | Sim | Não | Sim | Não |
| Ingressado no Azure AD Híbrido | Sim | Sim | Sim | Sim | Sim |
| Não ingressado no domínio | Sim | Sim | Não | Sim | Não |

## Provedores de identidade de autenticação de workspace compatíveis

| IDENTIDADE DA MÁQUINA | AZURE ACTIVE DIRECTORY | ACTIVE DIRECTORY | ACTIVE DIRECTORY E TOKEN | OKTA | SAML | CITRIX GATEWAY | AUTENTICAÇÃO ADAPTATIVA |
|---|---|---|---|---|---|---|---|
| Ingressado no AD | Sim | Sim | Sim | Sim | Sim | Sim | Sim |
| Ingressado no Azure AD | Sim | Não | Não | Não | Não | Não | Não |
| Ingressado no Azure | Sim | Sim | Sim | Sim | Sim | Sim | Sim |

| IDENTIDADE DA MÁQUINA | AZURE ACTIVE DIRECTORY | ACTIVE DIRECTORY | ACTIVE DIRECTORY E TOKEN | OKTA | SAML | CITRIX GATEWAY | AUTENTICAÇÃO ADAPTATIVA |
|---|---|---|---|---|---|---|---|
| AD Híbrido | | | | | | | |
| Não associado ao domínio | Sim | Sim | Sim | Sim | Sim | Sim | Sim |

## Associado ao Active Directory

O Active Directory é necessário para autenticação e autorização. A infraestrutura Kerberos no Active Directory é usada para garantir a autenticidade e a confidencialidade das comunicações com os Delivery Controllers. Para obter informações sobre o Kerberos, consulte a documentação da Microsoft.

O artigo Requisitos do sistema lista os níveis funcionais suportados para a floresta e o domínio. Para usar o Modelagem de Política, o controlador de domínio deve estar executando o Windows Server 2003 a Windows Server 2012 R2. Isso não afeta o nível funcional do domínio.

Este produto suporta:

- **Implantações nas quais as contas de usuário e as contas de computador existem em domínios em uma única floresta do Active Directory.** As contas de usuário e computador podem existir em domínios arbitrários dentro de uma única floresta. Todos os níveis funcionais de domínio e níveis funcionais de floresta são suportados neste tipo de implantação.
- **Implantações nas quais as contas de usuário existem em uma floresta do Active Directory diferente da floresta do Active Directory que contém as contas de computador dos Controllers e dos desktops virtuais.** Neste tipo de implantação, os domínios que contêm as contas de computador do Controller e do desktop virtual devem confiar nos domínios que contêm as contas de usuário. Podem ser usadas relações de confiança de floresta ou relações de confiança externas. Todos os níveis funcionais de domínio e níveis funcionais de floresta são suportados neste tipo de implantação.
- **Implantações nas quais as contas de computador para Controllers existem em uma floresta do Active Directory diferente de uma ou mais florestas adicionais do Active Directory que contêm as contas de computador dos desktops virtuais.** Neste tipo de

implantação, deve existir uma relação de confiança bidirecional entre os domínios que contêm as contas de computador do Controller e todos os domínios que contêm as contas de computador do desktop virtual. Neste tipo de implantação, todos os domínios que contêm contas de computador do Controller ou do desktop virtual devem estar no nível funcional "Windows 2000 nativo" ou superior. Todos os níveis funcionais de floresta são suportados.

- **Controladores de domínio graváveis.** Controladores de domínio somente leitura não são suportados.

Opcionalmente, os Virtual Delivery Agents (VDAs) podem usar informações publicadas no Active Directory para determinar com quais Controllers eles podem se registrar (descoberta). Este método é suportado principalmente para compatibilidade com versões anteriores e está disponível apenas se os VDAs estiverem na mesma floresta do Active Directory que os Controllers. Para obter informações sobre este método de descoberta, consulte Descoberta baseada em OU do Active Directory e CTX118976.

> **Observação:**
>
> Não altere o nome do computador ou a associação ao domínio de um Delivery Controller™ depois que o site for configurado.

### Implantar em um ambiente de várias florestas do Active Directory

Em um ambiente do Active Directory com várias florestas, se houver relações de confiança unidirecionais ou bidirecionais, você poderá usar encaminhadores DNS ou encaminhadores condicionais para pesquisa e registro de nomes. Para permitir que os usuários apropriados do Active Directory criem contas de computador, use o assistente de Delegação de Controle. Consulte a documentação da Microsoft para obter detalhes sobre este assistente.

Nenhuma zona DNS reversa é necessária na infraestrutura DNS se houver encaminhadores DNS apropriados entre as florestas.

A chave `SupportMultipleForest` é necessária se o VDA e o Controller estiverem em florestas separadas, independentemente de os nomes do Active Directory e NetBIOS serem diferentes. Use as informações a seguir para adicionar a chave do Registro ao VDA e aos Delivery Controllers:

> **Cuidado:**

> A edição incorreta do Registro 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. Faça backup do Registro antes de editá-lo.

> No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Em todos os Delivery Controllers, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Você pode precisar de configuração de DNS reverso se o seu namespace DNS for diferente do do Active Directory.

Uma entrada de registro foi adicionada para evitar a habilitação indesejada da autenticação NTLM em VDAs, que é menos segura que o Kerberos. Esta entrada pode ser usada em vez da entrada `SupportMultipleForest`, que ainda pode ser usada para compatibilidade com versões anteriores.

No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`.

- Nome: `SupportMultipleForestDdcLookup`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Esta chave de registro executa uma pesquisa DDC em um ambiente de múltiplas florestas com confiança bidirecional que permite remover a autenticação baseada em NTLM durante o processo de registro inicial.

Se houver trusts externos durante a configuração, a chave de registro `ListOfSIDs` é necessária. A chave de registro `ListOfSIDs` também é necessária se o FQDN do Active Directory for diferente do FQDN do DNS, ou se o domínio que contém o Domain Controller tiver um nome NetBIOS diferente do FQDN do Active Directory. Para adicionar a chave de registro, use as seguintes informações:

Para o VDA, localize a chave de registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`.

- Nome: `ListOfSIDs`
- Tipo: `REG_SZ`
- Dados: Identificador de Segurança (SID) dos Controladores. (SIDs estão incluídos nos resultados do cmdlet `Get-BrokerController`.)

Quando houver trusts externos, faça a seguinte alteração no VDA:

1. Localize o arquivo `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.
2. Faça uma cópia de backup do arquivo.
3. Abra o arquivo em um programa de edição de texto, como o Bloco de Notas.
4. Localize o texto `allowNtlm="false"` e altere o texto para `allowNtlm="true"`.
5. Salve o arquivo.

Após adicionar a chave de registro `ListOfSIDs` e editar o arquivo `brokeragent.exe.config`, reinicie o Serviço de Área de Trabalho Citrix para aplicar as alterações.

A tabela a seguir lista os tipos de confiança suportados:

| TIPO DE CONFIANÇA | TRANSITIVIDADE | DIREÇÃO | SUPORTADO NESTA VERSÃO |
|---|---|---|---|
| Pai e filho | Transitivo | Bidirecional | Sim |
| Raiz da árvore | Transitivo | Bidirecional | Sim |
| Externo | Não transitivo | Unidirecional ou bidirecional | Sim |
| Floresta | Transitivo | Unidirecional ou bidirecional | Sim |

| TIPO DE CONFIANÇA | TRANSITIVIDADE | DIREÇÃO | SUPORTADO NESTA VERSÃO |
|---|---|---|---|
| Atalho | Transitivo | Unidirecional ou bidirecional | Sim |
| Domínio | Transitivo ou não transitivo | Unidirecional ou bidirecional | Não |

Para obter mais informações sobre ambientes complexos do Active Directory, consulte CTX134971.

## Unido hibridamente ao Microsoft Entra

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

> Este artigo descreve os requisitos para criar um pool de identidades de catálogos híbridos do Microsoft Entra, além dos requisitos descritos na seção de requisitos do sistema.

Máquinas híbridas do Microsoft Entra usam o AD local como provedor de autenticação. Você pode atribuí-las a usuários ou grupos de domínio no AD local. Para habilitar a experiência de SSO contínuo do Azure AD, você precisa ter os usuários de domínio sincronizados com o Azure AD.

> **Observação:**
>
> VMs híbridas do Microsoft Entra são suportadas em infraestruturas de identidade federadas e gerenciadas.

### Requisitos

- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2212 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente

- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Qualquer hipervisor ou serviço de nuvem

### Limitações

- Se o Citrix Federated Authentication Service (FAS) for usado, o logon único será direcionado ao AD local em vez do Microsoft Entra ID. Neste caso, é recomendável configurar a autenticação baseada em certificado do Microsoft Entra para que o token de atualização primário (PRT) seja gerado no logon do usuário, o que facilita o logon único para recursos do Microsoft Entra dentro da sessão. Caso contrário, o PRT não estará presente e o SSO para recursos do Microsoft Entra não funcionará. Para obter informações sobre como obter o logon único (SSO) do Microsoft Entra para VDAs híbridos usando o Citrix Federated Authentication Service (FAS), consulte VDAs híbridos.
- Não pule a preparação da imagem ao criar ou atualizar catálogos de máquinas. Se você quiser pular a preparação da imagem, certifique-se de que as VMs mestre não sejam Microsoft Entra ou híbridas do Microsoft Entra.

### Considerações

- A criação de máquinas híbridas do Microsoft Entra requer a permissão `Write userCertificate` no domínio de destino. Certifique-se de inserir as credenciais de um administrador com essa permissão durante a criação do catálogo.
- O processo de junção híbrida do Microsoft Entra é gerenciado pela Citrix. Você precisa desabilitar `autoWorkplaceJoin` controlado pelo Windows nas VMs mestre da seguinte forma. A tarefa de desabilitar manualmente `autoWorkplaceJoin` é necessária apenas para a versão 2212 ou anterior do VDA.

  a. Execute `gpedit.msc`.

  b. navegar para **Configuração do Computador > Modelos Administrativos > Componentes do Windows > Registro de Dispositivo**.

  c. Defina **Registrar computadores ingressados no domínio como dispositivos** como **Desabilitado**.

- Selecione a Unidade Organizacional (OU) que está configurada para ser sincronizada com o Microsoft Entra ID ao criar as identidades da máquina.
- Para uma VM mestre baseada no Windows 11 22H2, crie uma tarefa agendada na VM mestre que execute os seguintes comandos na inicialização do sistema usando a conta SYSTEM.

Esta tarefa de agendar uma tarefa na VM mestre é necessária apenas para a versão 2212 ou anterior do VDA.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force
```

```
        Start-Sleep 5
        dsregcmd /join
        break
    }
  }


  Start-Sleep 1
}
```

- Por padrão, o Microsoft Entra Connect sincroniza a cada 30 minutos. As máquinas provisionadas podem levar até 30 minutos para serem ingressadas no Microsoft Entra híbrido durante a primeira inicialização.

### Próximos passos

Para obter mais informações sobre como criar um pool de identidades de catálogos ingressados no Microsoft Entra híbrido, consulte Pool de identidades de identidade de máquina ingressada no Microsoft Entra híbrido.

## Não associado a domínio

Este artigo descreve os requisitos para criar catálogos não associados a domínio usando o Citrix Virtual Apps and Desktops, além dos requisitos descritos na seção Requisitos do Sistema.

### Requisitos

- Plano de controle: Consulte Configurações Suportadas
- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2311 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Todas as plataformas suportadas pelo MCS
- O Rendezvous V2 deve estar ativado

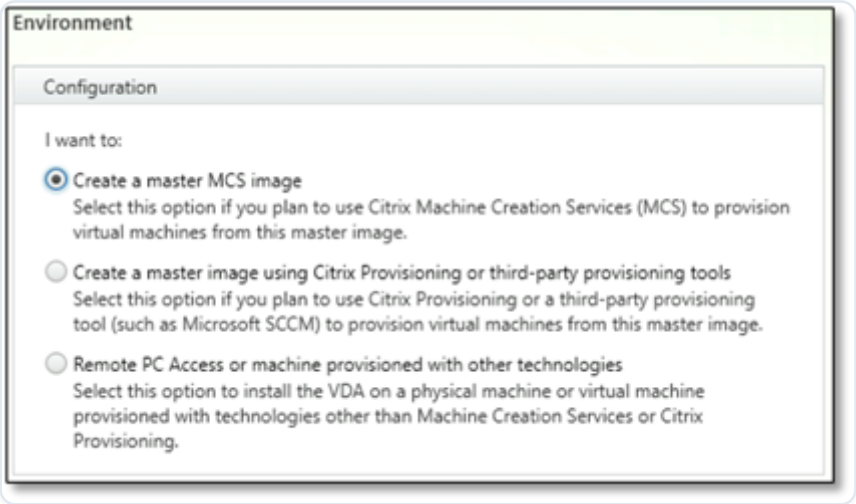
### Limitações

- A continuidade do serviço não é suportada.
- Sempre que usamos um VDA de várias sessões não associado a domínio, os dados de perfil do usuário local não são retidos e são excluídos ao fazer logoff.

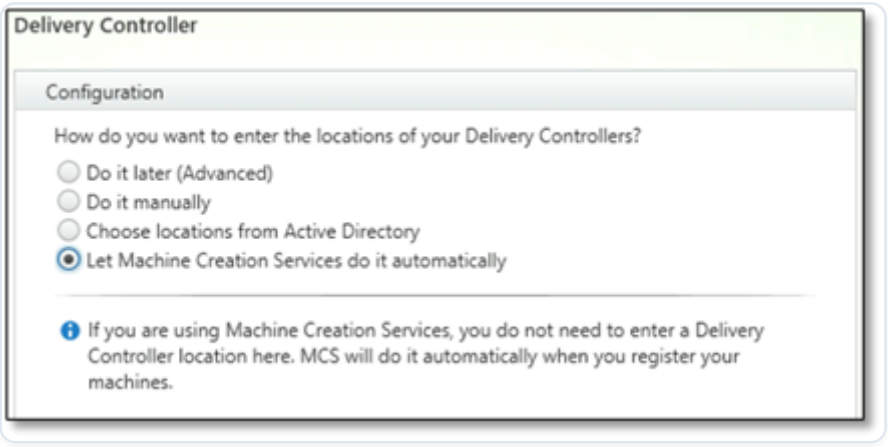
### Instalação e configuração do VDA

Siga as etapas para instalar o VDA:

1. Certifique-se de selecionar as seguintes opções no assistente de instalação:
    - Na página Ambiente, selecione **Criar uma imagem mestre MCS**.




    - Na página Delivery Controller™, selecione **Deixar o Machine Creation Services fazer isso automaticamente**.




### Próximos passos

Uma vez que o local do recurso e a conexão de hospedagem estejam disponíveis, prossiga para criar o pool de identidades. Para obter mais informações sobre como criar um pool de identidades

de máquinas não associadas a domínio, consulte Pool de identidades de máquinas não associadas a domínio.

# Preparar para instalar

A implantação do Citrix Virtual Apps and Desktops™ começa com a instalação dos seguintes componentes. Este processo prepara a entrega de aplicativos e desktops para usuários dentro do seu firewall.

- Um ou mais Delivery Controllers
- Citrix Director
- Citrix StoreFront™
- Citrix License Server
- Um ou mais Citrix Virtual Delivery Agents (VDAs)
- Componentes e tecnologias opcionais, como Universal Print Server, Federated Authentication Service e Self-Service Password Reset

Para usuários fora do seu firewall, instale e configure um componente extra, como o Citrix Gateway. Para uma introdução, consulte Integrar Citrix Virtual Apps and Desktops com Citrix Gateway.

> **Observação:**

> Certifique-se de que os seguintes pré-requisitos da Microsoft sejam atendidos no SO do servidor e no SO da estação de trabalho:

> - Os serviços **Volume Shadow Copy** e **Microsoft Software Shadow Copy Provider** da Microsoft estão em execução. Para obter mais informações, consulte Volume Shadow Copy Service.
> - A versão do **MS-Defender** deve ser superior a 4.18.2105.5. Para obter mais informações, consulte Atualizações de inteligência de segurança e produto do Microsoft Defender Antivirus.

> Se sua implantação incluir cargas de trabalho do Windows Server, configure um Microsoft RDS License Server.

Você pode usar o instalador completo do produto no ISO do produto para implantar muitos componentes e tecnologias. Você pode usar um instalador VDA autônomo para instalar VDAs. Os instaladores VDA autônomos estão disponíveis no site de download da Citrix. Todos os instaladores oferecem interfaces gráficas e de linha de comando. Consulte Instaladores.

O ISO do produto contém scripts de exemplo que instalam, atualizam ou removem VDAs para máquinas em um Active Directory. Você também pode usar os scripts para gerenciar imagens usadas pelo Machine Creation Services (MCS) e Citrix Provisioning (anteriormente Provisioning Services). Para obter detalhes, consulte Instalar VDAs usando scripts.

## Informações a serem revisadas antes da instalação

- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/technical-overview.html): Para se familiarizar com o produto e seus componentes.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/secure.html): Ao planejar seu ambiente de implantação.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/whats-new/known-issues.html): Problemas que você pode encontrar nesta versão.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/technical-overview/databases.html): Saiba mais sobre os bancos de dados do sistema e como configurá-los. Durante a instalação do Controller, você pode instalar o SQL Server Express para usar como banco de dados do site. A maioria das informações do banco de dados é configurada ao criar um site, após a instalação dos componentes principais.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/remote-pc-access.html): Se você estiver implantando um ambiente que permite que seus usuários acessem suas máquinas físicas no escritório remotamente.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html): Se você estiver usando um hipervisor ou outro serviço para hospedar ou provisionar VMs para aplicativos e desktops. Você pode configurar a primeira conexão ao criar um site (após a instalação dos componentes principais). Configure seu ambiente de virtualização antes disso.
- (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/configmgr.html): Se você estiver usando o ConfigMgr para gerenciar o acesso a aplicativos e desktops, ou se estiver usando o recurso Wake on LAN com o Remote PC Access.
- **Conexões de host de Nuvem Pública:** Se você tiver uma Licença de Direitos Híbridos, poderá criar conexões de host para a nuvem pública. Para obter informações relacionadas à Licença de Direitos Híbridos, consulte Renovações de Direitos Híbridos. Para obter

informações relacionadas ao direito à nuvem pública e os motivos para essa alteração, consulte CTX270373.

## Onde instalar os componentes

Revise os Requisitos do sistema para plataformas, sistemas operacionais e versões suportados. Os pré-requisitos dos componentes são instalados automaticamente, exceto quando indicado. Consulte a documentação do Citrix StoreFront e do Citrix License Server para suas plataformas e pré-requisitos suportados.

Você pode instalar os componentes principais no mesmo servidor ou em servidores diferentes.

- A instalação de todos os componentes principais em um único servidor pode funcionar para implantações de avaliação, teste ou pequenas produções.
- Para acomodar futuras expansões, considere instalar os componentes em servidores diferentes. Por exemplo, instalar o Studio em uma máquina diferente do servidor onde você instalou o Controller permite gerenciar o site remotamente.
- Para a maioria das implantações de produção, é recomendável instalar os componentes principais em servidores separados.

  Instale o Citrix License Server e as licenças antes de instalar outros componentes em outros servidores.
- Para instalar um componente compatível em um Server CoreOS (como um Delivery Controller), você deve usar a linha de comando. Esse tipo de SO não oferece uma interface gráfica, então instale o Studio e outras ferramentas em outro lugar e, em seguida, aponte-os para o servidor Controller.

Você pode instalar um Delivery Controller™ e um VDA para SO de várias sessões no mesmo servidor. Inicie o instalador e selecione o Delivery Controller (além de quaisquer outros componentes principais que você deseja nessa máquina). Em seguida, inicie o instalador novamente e selecione o **Virtual Delivery Agent** para SO de várias sessões.

Certifique-se de que cada sistema operacional tenha as atualizações mais recentes.

Certifique-se de que todas as máquinas tenham os relógios do sistema sincronizados. A infraestrutura Kerberos que protege a comunicação entre as máquinas requer sincronização.

Com XenServers, o estado de energia da máquina virtual pode aparecer como desconhecido, mesmo que pareça registrado. Para resolver esse problema, edite o valor da chave do Registro `HostTime` para desabilitar a sincronização de tempo com o host:

`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"`

`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"`

> **Dica:**
>
> O valor padrão é `HostTime="UTC"`. Altere este valor para algo diferente de UTC, por exemplo, `Local`. Essa alteração desabilita efetivamente a sincronização de tempo com o host.

> Orientações de otimização para máquinas Windows 10 de sessão única estão disponíveis em CTX216252.

Onde NÃO instalar componentes:

- Não instale nenhum componente em um controlador de domínio do Active Directory.
- Não há suporte para a instalação de um Controller em um nó em uma instalação de cluster do SQL Server, instalação de espelhamento do SQL Server ou em um servidor que executa o Hyper-V.

Se você tentar instalar ou atualizar um VDA em um sistema operacional Windows que esta versão do produto não suporta, uma mensagem o guiará para um artigo descrevendo as opções.

## Requisitos de Permissão e Active Directory

Você deve ser um usuário de domínio e um administrador local nas máquinas onde você está instalando os componentes.

Para usar um instalador VDA autônomo, você deve ter privilégios administrativos elevados ou usar **Executar como administrador**.

Configure seu domínio do Active Directory antes de iniciar uma instalação.

- Requisitos do sistema lista os níveis funcionais do Active Directory suportados. Active Directory unido contém mais informações.
- Você deve ter pelo menos um controlador de domínio executando os Serviços de Domínio do Active Directory.
- Não instale nenhum componente do Citrix Virtual Apps and Desktops em um controlador de domínio.

- Não use uma barra (/) ao especificar nomes de Unidades Organizacionais no Studio.

A conta de usuário do Windows usada para instalar o Citrix License Server é configurada automaticamente como um administrador completo de administração delegada.

Para mais informações:

- Melhores práticas de segurança
- Administração delegada
- Documentação da Microsoft para configuração do Active Directory

## Orientação de instalação, considerações e melhores práticas

### Durante a instalação de qualquer componente

- Ao instalar ou atualizar um Delivery Controller, Studio, License Server ou Director a partir da mídia do produto completo, se o instalador Citrix detectar que um reinício está pendente de uma instalação anterior do Windows na máquina, o instalador para com o código de saída/retorno 9. Você será solicitado a reiniciar a máquina.

  Este não é um reinício forçado pelo Citrix. É devido a outros componentes instalados anteriormente na máquina. Se isso ocorrer, reinicie a máquina e, em seguida, inicie o instalador Citrix novamente.

  Ao usar a interface de linha de comando, você pode evitar a verificação de reinício pendente incluindo a opção `/no_pending_reboot_check` no comando.
- Geralmente, se um componente tiver pré-requisitos, o instalador os implanta se não estiverem presentes. Alguns pré-requisitos podem exigir a reinicialização da máquina.
- Ao criar objetos antes, durante e após a instalação, especifique nomes exclusivos para cada objeto. Por exemplo, forneça nomes exclusivos para redes, grupos, catálogos e recursos.
- Se um componente não for instalado com êxito, a instalação será interrompida com uma mensagem de erro. Os componentes instalados com êxito são mantidos. Você não precisa reinstalá-los.
- Os Citrix Analytics são coletados automaticamente quando você instala (ou atualiza) componentes. Por padrão, esses dados são carregados para a Citrix automaticamente quando a instalação é concluída. Além disso, ao instalar componentes, você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix, que carrega dados anônimos.

Durante a instalação, você também pode optar por participar de outras tecnologias Citrix que coletam diagnósticos para manutenção e solução de problemas. Para obter informações sobre esses programas, consulte Citrix Insight Services.

- Os Google Analytics são coletados (e posteriormente carregados) automaticamente quando você instala (ou atualiza) o Studio. Após a instalação do Studio, você pode alterar essa configuração com a chave de registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Um valor de **1** habilita a coleta e o upload, **0** desabilita a coleta e o upload.
- Se uma instalação de VDA falhar, um analisador MSI analisa o log MSI com falha, exibindo o código de erro exato. O analisador sugere um artigo CTX, se for um problema conhecido. O analisador também coleta dados anonimizados sobre o código de erro da falha. Esses dados são incluídos com outros dados coletados pelo CEIP. Se você encerrar a inscrição no CEIP, os dados coletados pelo analisador MSI não serão mais enviados para a Citrix.

### Durante a instalação do VDA

- O Citrix Workspace™ app para Windows está disponível, mas não é instalado por padrão ao instalar um VDA. Você ou seus usuários podem baixar e instalar (e atualizar) o Citrix Workspace app para Windows e outros aplicativos Citrix Workspace no site da Citrix. Alternativamente, você pode disponibilizar esses aplicativos Citrix Workspace a partir do seu servidor StoreFront. Consulte a documentação do StoreFront.
- O Serviço de Spooler de Impressão da Microsoft deve estar habilitado. Você não pode instalar um VDA com êxito se esse serviço estiver desabilitado.
- A maioria das edições do Windows suportadas vem com o Microsoft Media Foundation já instalado. Se a máquina não tiver o Media Foundation (como as edições N), vários recursos multimídia não serão instalados e não funcionarão.
  - Redirecionamento de Mídia do Windows
  - Redirecionamento de Vídeo HTML5
  - Redirecionamento de Webcam HDX™ RealTime

  Você pode reconhecer a limitação ou encerrar a instalação do VDA e reiniciá-la mais tarde, após instalar o Media Foundation. Na interface gráfica, essa escolha é apresentada em uma mensagem. Na linha de comando, você pode usar a opção `/no_mediafoundation_ack` para reconhecer a limitação.
- Ao instalar o VDA, um novo grupo de usuários local chamado **Direct Access Users** é criado automaticamente. Em um VDA para SO de sessão única, este grupo se aplica apenas a

conexões RDP. Em um VDA para SO de múltiplas sessões, este grupo se aplica a conexões ICA® e RDP.

- O VDA deve ter endereços de Controller válidos para se comunicar. Caso contrário, as sessões não podem ser estabelecidas. Você pode especificar os endereços do Controller ao instalar o VDA ou posteriormente. Lembre-se de que isso deve ser feito. Para obter mais informações, consulte Registro do VDA.

### Reinicializações após e durante a instalação do VDA

É necessário reiniciar ao final da instalação do VDA. Essa reinicialização ocorre automaticamente por padrão.

Ao atualizar um VDA para a versão 7.17 (ou uma versão posterior suportada), ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Para minimizar o número de reinicializações necessárias durante a instalação do VDA:

- Certifique-se de que uma versão compatível do .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas com SO Windows multi-sessão, instale e habilite os serviços de função RDS antes de instalar o VDA.

Se você não instalar esses pré-requisitos antes de instalar o VDA:

- Se você estiver usando a interface gráfica ou a interface de linha de comando sem a opção `/noreboot`, a máquina reinicia automaticamente após a instalação do pré-requisito.
- Se você estiver usando a interface de linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Ao atualizar uma versão do VDA, ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

### Restaurar em caso de falha na instalação ou atualização

> **Nota:**
>
> Este recurso está disponível para VDAs de sessão única e multi-sessão.

> Se uma instalação ou atualização de VDA de sessão única falhar, e o recurso "restaurar em caso de falha" estiver habilitado, a máquina é retornada a um ponto de restauração que foi definido antes do início da instalação ou atualização.

Se uma instalação ou atualização de VDA multi-sessão falhar, e o recurso de "restauração em caso de falha" estiver habilitado, a máquina é retornada a um backup que foi realizado antes do início da instalação ou atualização.

Quando uma instalação ou atualização de VDA de sessão única é iniciada com este recurso habilitado, o instalador cria um ponto de restauração do sistema antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado do ponto de restauração. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração.

Quando uma instalação ou atualização de VDA multi-sessão é iniciada com este recurso habilitado, o instalador cria um backup do servidor antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado de backup. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração. O tempo para criar o backup do servidor é baseado no tamanho do backup necessário e na quantidade de recursos disponíveis para o servidor. O backup é armazenado em *C:\WindowsImageBackup\servername*.

Por padrão, este recurso está desativado.

Se você planeja ativar este recurso, certifique-se de que a restauração do sistema não esteja desativada por meio de uma configuração de GPO (`Computer Configuration > Administrative Templates > System > System Restore`).

> **Nota:**
>
> Esta configuração de GPO não se aplica à restauração de um VDA multi-sessão.

> Para habilitar este recurso ao instalar ou atualizar um VDA de sessão única ou multi-sessão:

- Ao usar a interface gráfica de um instalador VDA (como usando **Autostart** ou o comando `XenDesktopVDASetup.exe` sem quaisquer opções de restauração ou silenciosas), selecione a caixa de seleção **Habilitar restauração automática se a atualização falhar** na página **Resumo**.

Se a instalação/atualização for concluída com sucesso, o ponto de restauração/backup não é usado, mas é retido.

- Execute um instalador VDA com a opção `/enablerestore` ou `/enablerestorecleanup` usando a linha de comando.
  - Se você usar a opção `/enablerestorecleanup`, e a instalação/atualização for concluída com sucesso, o ponto de restauração/backup do servidor é removido automaticamente.
  - Se você usar a opção `/enablerestore`, e a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será retido.

## Instaladores

### Instalador do produto completo

Usando o instalador do produto completo fornecido na ISO, você pode:

- Instalar, atualizar ou remover componentes principais: Delivery Controller, Studio, Director e License Server.
- Instalar ou atualizar o StoreFront.
- Instalar ou atualizar VDAs Windows para sistemas operacionais de sessão única ou multi-sessão.
- Instale o componente `UpsServer` do Universal Print Server em seus servidores de impressão.
- Instale o Federated Authentication Service.
- Instale o Session Recording.
- Instale o Workspace Environment Management.

> **Nota:**
>
> O instalador do agente do Workspace Environment Management™ não está localizado. Ele está disponível apenas em inglês.

Para entregar um desktop de um SO multi-sessão para um usuário (por exemplo, para desenvolvimento web), use a interface de linha de comando do instalador completo do produto. Para obter detalhes, consulte Server VDI.

### Instaladores VDA autônomos

Os instaladores VDA autônomos estão disponíveis nas páginas de download da Citrix. (Eles não estão disponíveis na mídia de instalação do produto.) Os instaladores VDA autônomos são muito menores do que o ISO completo do produto. Eles acomodam mais facilmente implantações que:

- Usam pacotes de Distribuição Eletrônica de Software (ESD) que são preparados ou copiados localmente
- Têm máquinas físicas
- Têm escritórios remotos

Por padrão, os arquivos nos VDAs autônomos autoextraíveis são extraídos para a pasta **Temp**. É necessário mais espaço em disco na máquina ao extrair para a pasta **Temp** do que ao usar o instalador completo do produto. No entanto, os arquivos extraídos para a pasta **Temp** são automaticamente excluídos após a conclusão da instalação. Alternativamente, você pode usar o comando `/extract` com um caminho absoluto.

Três instaladores VDA autônomos estão disponíveis para download.

**VDAServerSetup.exe:**

Instala um VDA para SO multi-sessão. Ele suporta todas as opções de VDA para SO multi-sessão que estão disponíveis com o instalador do produto completo.

**VDAWorkstationSetup.exe:**

Instala um VDA para SO de sessão única. Ele suporta todas as opções de VDA para SO de sessão única que estão disponíveis com o instalador do produto completo.

**VDAWorkstationCoreSetup.exe:**

Instala um VDA para SO de sessão única que é otimizado para implantações de Acesso Remoto a PC ou instalações VDI principais. O Acesso Remoto a PC usa máquinas físicas. As instalações VDI principais são VMs que não estão sendo usadas como uma imagem. Ele instala apenas os serviços essenciais necessários para conexões VDA nessas implantações. Portanto, ele suporta apenas um subconjunto das opções que são válidas com os instaladores do produto completo ou `VDAWorkstationSetup.exe`.

Este instalador não instala nem contém os componentes usados para:

- App-V.

- Profile Management. Excluir o Citrix Profile Management da instalação afeta as exibições do Citrix Director. Para obter detalhes, consulte Instalar VDAs.
- Machine Identity Service.
- Citrix Supportability Tools.
- Citrix Files para Windows.
- Citrix Files para Outlook.

O instalador `VDAWorkstationCoreSetup.exe` não instala nem contém um Citrix Workspace app para Windows.

Usar `VDAWorkstationCoreSetup.exe` é equivalente a usar o instalador do produto completo ou `VDAWorkstationSetup` para instalar um VDA de SO de sessão única e uma das seguintes opções:

- Na interface gráfica: Selecionar a opção Acesso Remoto a PC na página **Ambiente**.
- Na interface de linha de comando: Especificando a opção `/remotepc`.
- Na interface de linha de comando: Especificando `/components vda` mais a opção `/exclude` que lista todos os nomes de componentes adicionais válidos.

Você pode instalar os componentes/recursos omitidos posteriormente executando o instalador completo do produto. Essa ação permite instalar todos os componentes ausentes.

O instalador `VDAWorkstationCoreSetup.exe` instala automaticamente o MSI de Redirecionamento de Conteúdo do Navegador. Essa instalação automática se aplica à versão 2003 do VDA e versões posteriores compatíveis.

## Códigos de retorno de instalação do Citrix

O log de instalação contém o resultado das instalações de componentes como um código de retorno do Citrix, não um valor da Microsoft.

- 0 = Sucesso
- 1 = Falha
- 2 = SucessoParcial
- 3 = SucessoParcialEReInicializaçãoNecessária
- 4 = FalhaEReInicializaçãoNecessária
- 5 = UsuárioCancelou

- 6 = ArgumentoDeLinhaDeComandoAusente
- 7 = VersãoMaisRecenteEncontrada
- 8 = SucessoReInicializaçãoNecessária
- 9 = FileLockReboot
- 10 = Abortado
- 11 = FailedMedia
- 12 = FailedLicense
- 13 = FailedPrecheck
- 14 = AbortedPendingRebootCheck
- -1 = Sair

Por exemplo, ao usar ferramentas como o Microsoft System Center Configuration Manager, uma instalação de VDA por script pode parecer falhar quando o log de instalação contém o código de retorno 3. Isso pode ocorrer quando o instalador do VDA está aguardando uma reinicialização que você deve iniciar (por exemplo, após uma instalação de pré-requisito de função RDS em um servidor). Uma instalação de VDA é considerada bem-sucedida somente depois que todos os pré-requisitos e componentes selecionados são instalados e a máquina é reiniciada após a instalação.

Alternativamente, você pode envolver sua instalação em scripts CMD (que retornam códigos de saída da Microsoft) ou alterar os códigos de sucesso em seu pacote do Configuration Manager.

## Configurar um Servidor de Licenças RDS da Microsoft para cargas de trabalho do Windows Server

Este produto acessa os recursos de sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2016. Isso geralmente requer uma licença de acesso para cliente dos Serviços de Área de Trabalho Remota (RDS CAL). O VDA deve ser capaz de contatar um servidor de licenças RDS para solicitar RDS CALs. Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento da Microsoft Ativar o Servidor de Licenças dos Serviços de Área de Trabalho Remota. Para ambientes de prova de conceito, você pode usar o período de carência fornecido pela Microsoft.

Com este método, você pode fazer com que este serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações de Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft Licenciar sua implantação RDS com licenças de acesso para cliente (CALs).

Para configurar o servidor de licenças RDS usando as configurações de Política de Grupo:

1. Instale um Servidor de Licenças dos Serviços de Área de Trabalho Remota em uma máquina disponível. A máquina deve estar sempre disponível. As cargas de trabalho do produto Citrix devem ser capazes de alcançar este servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para detalhes, consulte o documento da Microsoft Especificar o Modo de Licenciamento da Área de Trabalho Remota para um Servidor Host da Sessão RD.

As cargas de trabalho do Windows 10 exigem ativação de licença apropriada do Windows 10. Recomendamos que você siga a documentação da Microsoft para ativar cargas de trabalho do Windows 10.

## Mais informações

Para configurar o local do recurso para tipos de host específicos:

- Ambientes de nuvem AWS
- Ambientes de virtualização XenServer
- Ambientes do Google Cloud
- Ambientes de nuvem do Microsoft Azure Resource Manager
- Ambientes do Microsoft System Center Configuration Manager
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix
- Ambientes de virtualização VMware
- Soluções de nuvem e parceiros VMware

## Ambientes de nuvem AWS

Este artigo o orienta na configuração de sua conta AWS como um local de recurso que você pode usar com o Citrix Virtual Apps and Desktops. O local de recurso inclui um conjunto básico de componentes, ideal para uma prova de conceito ou outra implantação que não exija recursos espalhados por várias zonas de disponibilidade. Depois de concluir essas tarefas, você pode instalar VDAs, provisionar máquinas, criar catálogos de máquinas e criar Delivery Groups.

Ao concluir as tarefas neste artigo, seu local de recurso inclui os seguintes componentes:

- Uma nuvem privada virtual (VPC) com sub-redes públicas e privadas dentro de uma única zona de disponibilidade.
- Uma instância que funciona como um Controlador de Domínio do Active Directory e servidor DNS, localizada na sub-rede privada da VPC.
- Uma instância que atua como um host bastion na sub-rede pública da sua VPC. Esta instância é usada para iniciar conexões RDP com as instâncias na sub-rede privada para fins de administração. Depois de concluir a configuração do seu local de recurso, você pode desligar esta instância para que ela não seja mais facilmente acessível. Quando você precisar gerenciar outras instâncias na sub-rede privada, como instâncias VDA, você pode reiniciar a instância do host bastion.

### Visão geral da tarefa

**Configure uma nuvem privada virtual (VPC) com sub-redes públicas e privadas.** Ao concluir esta tarefa, a AWS implanta um gateway NAT com um endereço IP Elástico na sub-rede pública. Esta ação permite que as instâncias na sub-rede privada acessem a Internet. As instâncias na sub-rede pública são acessíveis ao tráfego público de entrada, enquanto as instâncias na sub-rede privada não são.

**Configurar grupos de segurança**. Os grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também associa esses grupos de segurança a cada instância em sua VPC.

**Crie um conjunto de opções DHCP**. Com uma VPC da Amazon, os serviços DHCP e DNS são fornecidos por padrão, o que afeta como você configura o DNS em seu Controlador de Domínio do Active Directory. O DHCP da Amazon não pode ser desativado e o DNS da Amazon pode ser usado apenas para resolução de DNS público, não para resolução de nomes do Active Directory. Para especificar o domínio e os servidores de nomes entregues às instâncias via DHCP, crie um conjunto de opções DHCP. O conjunto atribui o sufixo de domínio do Active Directory e especifica o servidor DNS para todas as instâncias em sua VPC. Para garantir que os registros Host (A) e Reverse Lookup (PTR) sejam registrados automaticamente quando as instâncias ingressarem no domínio, você configura as propriedades do adaptador de rede para cada instância que você adiciona à sub-rede privada.

**Adicione um host bastion e um Controlador de Domínio à VPC**. Através do host bastion, você pode fazer logon em instâncias na sub-rede privada para configurar o domínio e ingressar instâncias no domínio.

### Tarefa 1: Configurar a VPC

1. No console de gerenciamento da AWS, selecione **VPC**.
2. No Painel da VPC, selecione **Criar VPC**.
3. Selecione **VPC e mais**.
4. Em NAT gateways ($), selecione **Em 1 AZ** ou **1 por AZ**.
5. Em opções de DNS, deixe **Habilitar nomes de host DNS** selecionado.
6. Selecione **Criar VPC**. A AWS cria as sub-redes públicas e privadas, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

### Tarefa 2: Configurar grupos de segurança

Esta tarefa cria e configura os seguintes grupos de segurança para sua VPC:

- Um grupo de segurança público para associar às instâncias em sua sub-rede pública.
- Um grupo de segurança privado para associar às instâncias em sua sub-rede privada.

Para criar os grupos de segurança:

1. No Painel da VPC, selecione **Grupos de Segurança**.
2. Crie um grupo de segurança para o grupo de segurança público. Selecione **Criar Grupo de Segurança** e insira uma tag de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Sim, Criar**.

#### Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

| TIPO | ORIGEM |
|---|---|
| TODO o Tráfego | Selecione o grupo de segurança Privado. |
| TODO o Tráfego | Selecione o grupo de segurança Público. |
| ICMP | 0.0.0.0/0 |
| 22 (SSH) | 0.0.0.0/0 |
| 80 (HTTP) | 0.0.0.0/0 |

| TIPO | ORIGEM |
|---|---|
| 443 (HTTPS) | 0.0.0.0/0 |
| 1494 (ICA/HDX) | 0.0.0.0/0 |
| 2598 (Confiabilidade da Sessão) | 0.0.0.0/0 |
| 3389 (RDP) | 0.0.0.0/0 |

3. Quando terminar, selecione **Salvar**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

| TIPO | DESTINO |
|---|---|
| TODO o Tráfego | Selecione o grupo de segurança Privado. |
| TODO o Tráfego | 0.0.0.0/0 |
| ICMP | 0.0.0.0/0 |

5. Quando terminar, selecione **Salvar**.

**Configurar o grupo de segurança privado**

1. Na lista de grupos de segurança, selecione o grupo de segurança Privado.
2. Se você não configurou o tráfego do grupo de segurança público, você deve definir as portas TCP; selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

| TIPO | ORIGEM |
|---|---|
| TODO o Tráfego | Selecione o grupo de segurança Privado. |
| TODO o Tráfego | Selecione o grupo de segurança Público. |
| ICMP | Selecione o grupo de segurança Público. |
| TCP 53 (DNS) | Selecione o grupo de segurança Público. |
| UDP 53 (DNS) | Selecione o grupo de segurança Público. |
| 80 (HTTP) | Selecione o grupo de segurança Público. |

| TIPO | ORIGEM |
|---|---|
| TCP 135 | Selecione o grupo de segurança Público. |
| TCP 389 | Selecione o grupo de segurança Público. |
| UDP 389 | Selecione o grupo de segurança Público. |
| 443 (HTTPS) | Selecione o grupo de segurança Público. |
| TCP 1494 (ICA/HDX) | Selecione o grupo de segurança Público. |
| TCP 2598 (Confiabilidade da Sessão) | Selecione o grupo de segurança Público. |
| 3389 (RDP) | Selecione o grupo de segurança Público. |
| TCP 49152–65535 | Selecione o grupo de segurança Público. |

3. Quando terminar, selecione **Salvar.**
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

| TIPO | DESTINO |
|---|---|
| TODO o Tráfego | Selecione o grupo de segurança Privado. |
| TODO o Tráfego | 0.0.0.0/0 |
| ICMP | 0.0.0.0/0 |
| UDP 53 (DNS) | 0.0.0.0/0 |

5. Quando terminar, selecione **Salvar**.

### Tarefa 3: Iniciar instâncias

Siga os passos abaixo para criar duas instâncias EC2 e descriptografar a senha de Administrador padrão que a Amazon gera:

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No Painel do EC2, selecione **Iniciar Instância**.
3. Selecione uma imagem de máquina do Windows Server e o tipo de instância.

4. Na página **Configure Instance Details**, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Sub-rede**, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione a sub-rede Pública
    - Controlador de Domínio: Selecione a sub-rede Privada
6. Em **Atribuir automaticamente endereço IP público**, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione **Enable.**
    - Controlador de Domínio: Selecione **Use default setting** ou **Disable**.
7. Em **Network Interfaces**, insira um endereço IP primário dentro do intervalo de IP da sua sub-rede privada para o Controlador de Domínio.
8. Se necessário, na página **Adicionar Armazenamento**, modifique o tamanho do disco.
9. Na página **Marcar Instância**, insira um nome amigável para cada instância.
10. Na página **Configurar Grupos de Segurança**, selecione **Selecionar um grupo de segurança existente** e, em seguida, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione o grupo de segurança Público.
    - Controlador de Domínio: Selecione o grupo de segurança Privado.
11. Revise suas seleções e, em seguida, selecione **Iniciar**.
12. Crie um novo par de chaves ou selecione um existente. Se você criar um novo par de chaves, baixe seu arquivo de chave privada (.pem) e mantenha-o em um local seguro. Você deve fornecer sua chave privada ao adquirir a senha padrão do Administrador para a instância.
13. Selecione **Launch Instances**. Selecione **View Instances** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-lançada tenha passado por todas as verificações de status antes de acessá-la.
14. Adquira a senha padrão do Administrador para cada instância:
    a. Na lista de instâncias, selecione a instância e, em seguida, selecione **Conectar**.
    b. Vá para a guia **Cliente RDP**, selecione **Obter Senha** e carregue seu arquivo de chave privada (`.pem`) quando solicitado.
    c. Selecione **Descriptografar Senha** para obter a senha legível. A AWS exibe a senha padrão.

15. Repita as etapas do passo 2 até ter criado duas instâncias:
    - Uma instância de host bastion em sua sub-rede pública
    - Uma instância em sua sub-rede privada que será usada como Controlador de Domínio.

### Tarefa 4: Criar um conjunto de opções DHCP

1. No Painel da VPC, selecione **Conjuntos de Opções DHCP**.
2. Insira as seguintes informações:
    - Tag de nome: Insira um nome amigável para o conjunto.
    - Nome de domínio: Insira o nome de domínio totalmente qualificado que você usa ao configurar a instância do Controlador de Domínio.
    - Servidores de nome de domínio: Insira o endereço IP privado que você atribuiu à instância do Controlador de Domínio e a string **AmazonProvidedDNS**, separados por vírgulas.
    - Servidores NTP: Deixe este campo em branco.
    - Servidores de nome NetBIOS: Insira o endereço IP privado da instância do Controlador de Domínio.
    - Tipo de nó NetBIOS: Insira **2**.
3. Selecione **Sim, Criar.**
4. Associe o novo conjunto à sua VPC:
    a. No Painel da VPC, selecione **Suas VPCs** e, em seguida, selecione a VPC que você configurou anteriormente.
    b. Selecione **Ações > Editar Conjunto de Opções DHCP**.
    c. Quando solicitado, selecione o novo conjunto que você criou e, em seguida, selecione **Salvar**.

### Tarefa 5: Configurar as instâncias

1. Usando um cliente RDP, conecte-se ao endereço IP público da instância do host bastion. Quando solicitado, insira as credenciais da conta de Administrador.
2. Na instância do host bastion, inicie a Conexão de Área de Trabalho Remota e conecte-se ao endereço IP privado da instância que você deseja configurar. Quando solicitado, insira as credenciais de Administrador para a instância.
3. Para todas as instâncias na sub-rede privada, configure as configurações de DNS:

a. Selecione **Iniciar > Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento > Alterar configurações do adaptador**. Clique duas vezes na conexão de rede exibida.

b. Selecione **Propriedades > Protocolo de Internet Versão 4 (TCP/IPv4) > Propriedades**.

c. Selecione **Avançado > DNS**. Certifique-se de que as seguintes configurações estejam ativadas e selecione **OK**:

- Registrar os endereços desta conexão no DNS
- Usar o sufixo DNS desta conexão no registro DNS

4. Para configurar o Controlador de Domínio:

a. Usando o Gerenciador de Servidores, adicione a função Serviços de Domínio Active Directory com todos os recursos padrão.

b. Promova a instância a um Controlador de Domínio. Durante a promoção, habilite o DNS e use o nome de domínio que você especificou ao criar o conjunto de opções DHCP. Reinicie a instância quando solicitado.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão no AWS, consulte Conexão com o AWS

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

## Ambientes do Google Cloud

O Citrix Virtual Apps and Desktops™ permite provisionar e gerenciar máquinas no Google Cloud.

### Requisitos

- Conta do Citrix Cloud™. O recurso descrito neste artigo está disponível apenas no Citrix Cloud.
- Um projeto do Google Cloud. O projeto armazena todos os recursos de computação associados ao catálogo de máquinas. Pode ser um projeto existente ou um novo.

- Habilite quatro APIs em seu projeto do Google Cloud. Para obter detalhes, consulte Habilitar APIs do Google Cloud.
- Conta de serviço do Google Cloud. A conta de serviço autentica-se no Google Cloud para permitir o acesso ao projeto. Para obter detalhes, consulte Configurar e atualizar contas de serviço.
- Habilite o acesso privado do Google. Para obter detalhes, consulte Habilitar acesso privado do Google.

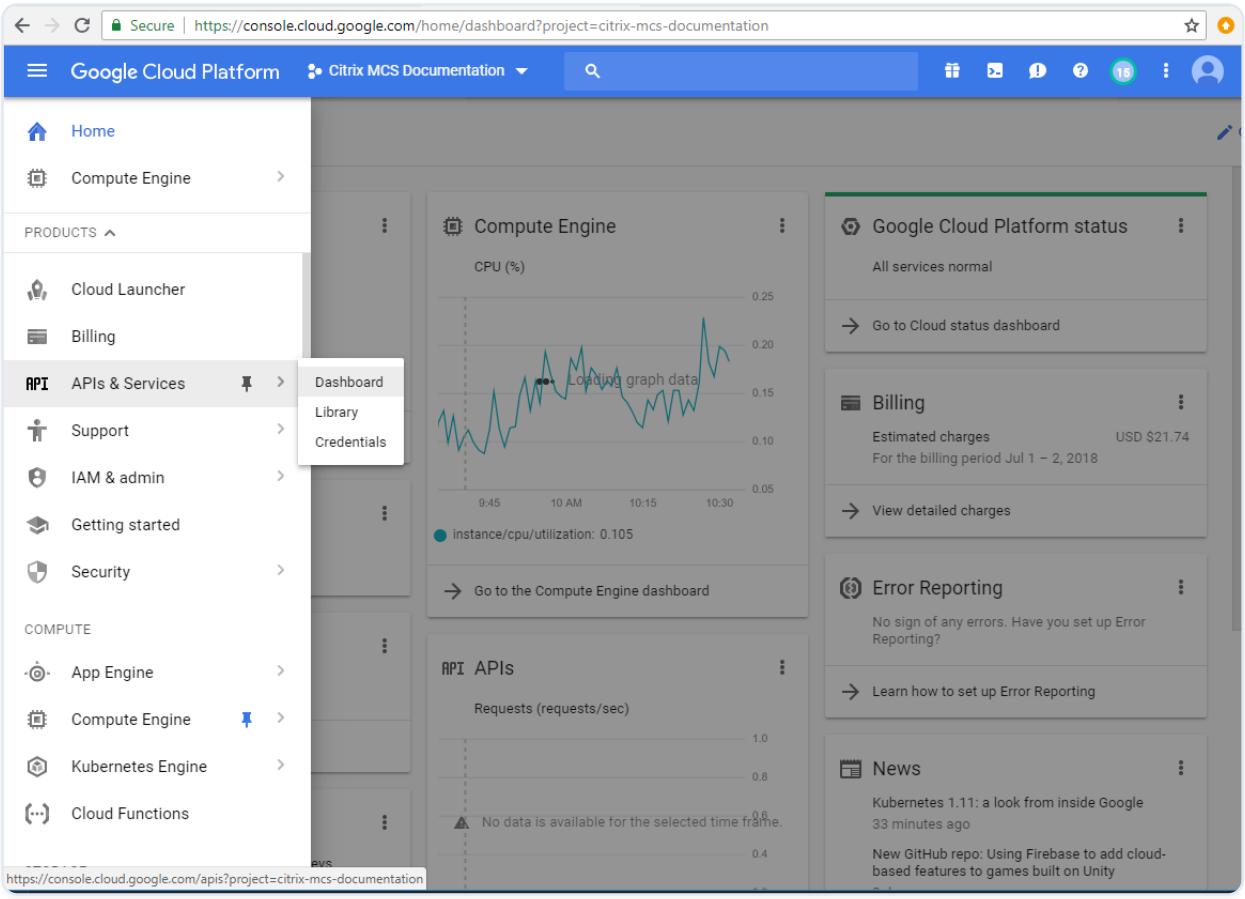
### Habilitar APIs do Google Cloud

Para usar a funcionalidade do Google Cloud através do Web Studio, habilite estas APIs em seu projeto do Google Cloud:

- Compute Engine API
- Cloud Resource Manager API
- API de Gerenciamento de Identidade e Acesso (IAM)
- Cloud Build API
- Cloud Key Management Service (KMS)

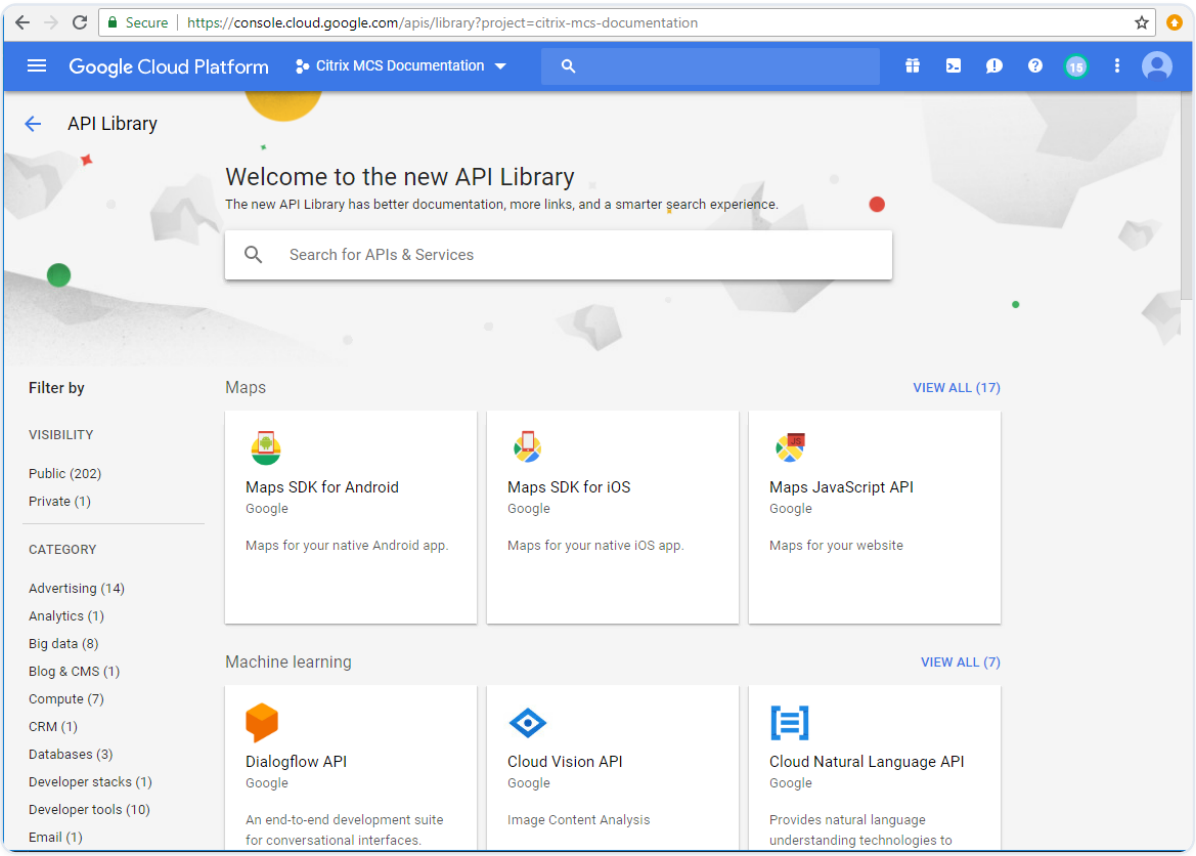
No console do Google Cloud, conclua estas etapas:

1. No menu superior esquerdo, selecione **APIs e Serviços > Painel**.




2. Na tela **Painel**, certifique-se de que a API do Compute Engine esteja habilitada. Caso contrário, siga estas etapas:

   a. navegar para **APIs and Services > Library**.




b. Na caixa de pesquisa, digite *Compute Engine*.

c. Nos resultados da pesquisa, selecione **Compute Engine API**.

d. Na página **Compute Engine API**, selecione **Enable**.

3. Ative a API do Cloud Resource Manager.

a. navegar para **APIs and Services > Library**.

b. Na caixa de pesquisa, digite *Cloud Resource Manager*.

c. Nos resultados da pesquisa, selecione **Cloud Resource Manager API**.

d. Na página **Cloud Resource Manager API**, selecione **Enable**. O status da API é exibido.

4. Da mesma forma, habilite a **API Identity and Access Management (IAM)** e a **API Cloud Build**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para fazer isso:

1. Abra o Google Console e carregue o Cloud Shell.
2. Execute os quatro comandos a seguir no Cloud Shell:

- gcloud services enable compute.googleapis.com.
- gcloud serviços habilitar cloudresourcemanager.googleapis.com

- gcloud serviços habilitar iam.googleapis.com
- gcloud serviços habilitar cloudbuild.googleapis.com

3. Clique em **Autorizar** se o Cloud Shell solicitar.

### Configurar e atualizar contas de serviço

> **Nota:**
>
> O GCP está introduzindo mudanças no comportamento padrão do Serviço Cloud Build e no uso de contas de serviço após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build habilitada antes de April 29, 2024 não são afetados por esta mudança. No entanto, se você quiser manter o comportamento existente do Serviço Cloud Build após April 29, você pode criar ou aplicar a política da organização para desabilitar a imposição da restrição antes de habilitar a API Cloud Build. Como resultado, o conteúdo a seguir é dividido em dois: Antes de April 29, 2024 e Depois de April 29, 2024. Se você definir a nova política da organização, siga a seção Antes de April 29, 2024.

#### Antes de April 29, 2024

O Citrix Cloud usa três contas de serviço separadas no projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente conforme descrito aqui. Para obter mais informações, consulte Criar uma Conta de Serviço do Citrix Cloud.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Conta de Serviço do Cloud Build*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Administrador > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**.

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **cloudbuild**. Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

Verifique se a conta de serviço recebeu as seguintes funções. Se você precisar adicionar funções, siga as etapas descritas em Adicionar funções à conta de serviço do Cloud Build.

- Conta de Serviço do Cloud Build
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é adicionada pelo Google Cloud às instâncias criadas no Google Cloud assim que a API Compute é ativada. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar uma função de **Administrador de Armazenamento** que requer as seguintes permissões:
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`.

### CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

   Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore
- Cloud KMS Crypto Operator

O Cloud KMS Crypto Operator requer as seguintes permissões:

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

**Considerações:**

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.

- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

### CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da conta de serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado e salvo automaticamente na pasta **Downloads** depois que você cria a chave. Ao criar a chave, certifique-se de definir o tipo de chave como JSON. Caso contrário, o Web Studio não poderá analisá-la.

Para criar uma chave de conta de serviço, navegar para **IAM e Administrador > Contas de serviço** e clique no endereço de e-mail da conta de serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

> **Dica:**
>
> Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

### ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

### ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CLOUD BUILD

Para adicionar funções à conta de serviço do Cloud Build:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a conta de serviço do Cloud Build, identificável por um endereço de e-mail que começa com o **ID do projeto** e a palavra **cloudbuild**.

   Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

   > **Nota:**
   >
   > Habilite todas as APIs para obter a lista completa de funções.

**Após April 29, 2024**

O Citrix Cloud usa duas contas de serviço separadas dentro do projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Admin > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar a função de **Administrador de Armazenamento** que requer as seguintes permissões:
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get

- storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com.`.

Verifique se a conta de serviço recebeu as seguintes funções.

- Conta de Serviço do Cloud Build
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

### CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

   Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

   - Administrador de Computação
   - Administrador de Armazenamento
   - Editor do Cloud Build
   - Usuário da Conta de Serviço
   - Usuário do Cloud Datastore
   - Cloud KMS Crypto Operator

   O Cloud KMS Crypto Operator requer as seguintes permissões:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get

- cloudkms.keyRings.list

> **Nota:**
>
> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

**Considerações:**

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.
- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

### CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da conta de serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado e salvo automaticamente na pasta **Downloads** depois que você cria a chave. Ao criar a chave, certifique-se de definir o tipo de chave como JSON. Caso contrário, o Web Studio não poderá analisá-la.

Para criar uma chave de conta de serviço, navegar para **IAM e Administrador > Contas de serviço** e clique no endereço de e-mail da conta de serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

**Dica:**

Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

### ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

### ADICIONAR PAPÉIS À CONTA DE SERVIÇO DO CLOUD COMPUTE

Para adicionar papéis à Conta de Serviço do Cloud Compute:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a Conta de Serviço do Cloud Compute, identificável por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**.

   Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

**Nota:**

Habilite todas as APIs para obter a lista completa de papéis.

### Permissões de armazenamento e gerenciamento de bucket

O Citrix Virtual Apps and Desktops aprimora o processo de relatório de falhas de build na nuvem para o serviço Google Cloud. Este serviço executa builds no Google Cloud. O Citrix Virtual Apps and Desktops cria um bucket de armazenamento chamado `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` onde os serviços do Google Cloud capturam informações de log de build. Uma opção é definida neste bucket que exclui o conteúdo após um período de 30 dias. Esse processo exige que a conta de serviço usada para a conexão tenha as permissões do Google Cloud definidas como `storage.buckets.update`. Se a conta de serviço não tiver essa permissão, o Citrix Virtual Apps and Desktops ignorará os erros e prosseguirá com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de build aumenta e exige limpeza manual.

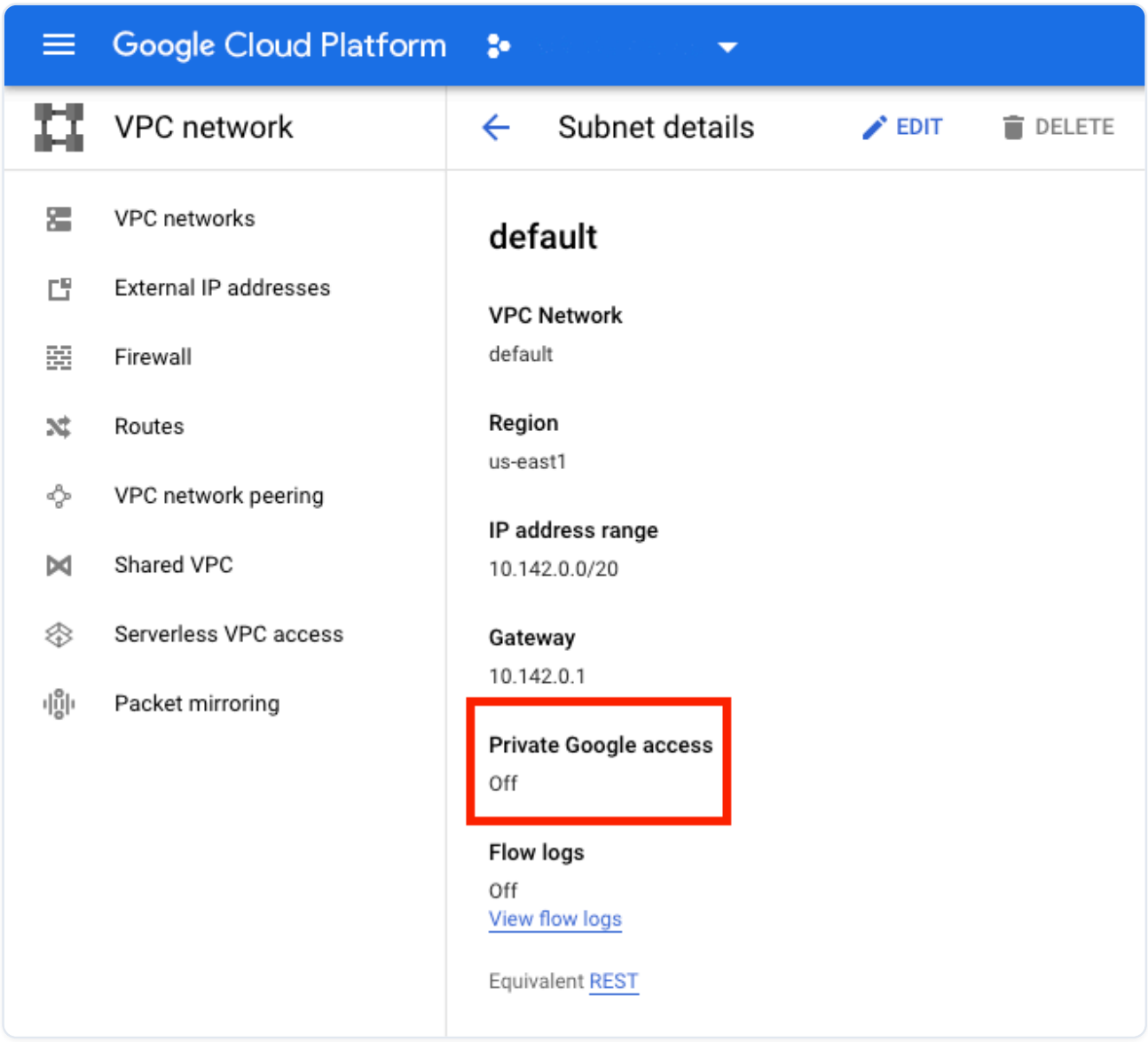
## Habilitar acesso privado do Google

Quando uma VM não possui um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Ao habilitar o acesso privado, a VM se conecta ao conjunto de endereços IP externos usados pela API do Google e serviços associados.

> **Nota:**
>
> Independentemente de o acesso privado do Google estar habilitado, todas as VMs, com e sem endereços IP públicos, devem ser capazes de acessar as APIs Públicas do Google, especialmente se dispositivos de rede de terceiros tiverem sido instalados no ambiente.

Para garantir que uma VM em sua sub-rede possa acessar as APIs do Google sem um endereço IP público para provisionamento MCS:

1. No Google Cloud, acesse a **configuração de rede VPC**.
2. Na tela de detalhes da sub-rede, ative o **Acesso privado do Google**.




Para obter mais informações, consulte Configurando o Acesso Privado do Google.

> **Importante:**
>
> Se sua rede estiver configurada para impedir o acesso da VM à Internet, certifique-se de que sua organização assuma os riscos associados à habilitação do Acesso privado do Google para a sub-rede à qual a VM está conectada.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site

- Para criar e gerenciar uma conexão em ambientes Google Cloud, consulte Conexão com ambientes Google Cloud

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)

## Ambientes de virtualização HPE Moonshot

O Citrix Virtual Apps and Desktops™ gerencia suas cargas de trabalho HPE Moonshot por meio de um plug-in HPE Moonshot gerenciado pela Citrix. Com este plug-in, você pode criar conexões para seus chassis HPE Moonshot, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo.

### Requisito

Instale o plug-in HPE Moonshot gerenciado pela Citrix no Delivery Controller.

**Nota:**

- Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, o Delivery Controller usará o plug-in HPE Moonshot gerenciado pela Citrix.
- Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, e você quiser usar o plug-in Moonshot gerenciado pela HPE, desinstale o plug-in HPE Moonshot gerenciado pela Citrix e atualize o cache `RegisterPlugin`.

#### Instalar o plug-in HPE Moonshot gerenciado pela Citrix

Para instalar o plug-in HPE Moonshot gerenciado pela Citrix, faça o seguinte:

1. Instale `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi. `E:\` é o ISO.
2. Abra o PowerShell como Administrador e execute o seguinte comando.

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. Após o registro bem-sucedido do plug-in, reinicie os seguintes serviços no **Gerenciador de Tarefas**:
   a. CitrixBrokerService
   b. CitrixHostService
   c. CitrixMachineCreationService
4. Execute `Get-HypHypervisorPlugins` para verificar se o plug-in está instalado no Delivery Controller. O campo **DisplayName** na saída deve ser exibido como **HPE Moonshot**.

**Desinstalar o plug-in HPE Moonshot gerenciado pela Citrix e atualizar o cache RegisterPlugin**

Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, e você quiser usar o plug-in Moonshot gerenciado pela HPE, você deve desinstalar o plug-in HPE Moonshot gerenciado pela Citrix e atualizar o cache `RegisterPlugin`. Para fazer isso:

1. Desinstale o plug-in HPE Moonshot gerenciado pelo Citrix.
2. Abra o PowerShell como Administrador e execute o seguinte comando:

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. Após o registro bem-sucedido do plug-in, reinicie os seguintes serviços a partir do **Gerenciador de Tarefas**:
   a. CitrixBrokerService
   b. CitrixHostService
   c. CitrixMachineCreationService
4. Execute `Get-HypHypervisorPlugins` para verificar se o plug-in está instalado no Delivery Controller. O campo **DisplayName** na saída deve aparecer como **HPE Moonshot Machine Manager**.

### Etapas principais

1. Configure seus ambientes HPE.
2. Crie uma conexão com o chassi HPE Moonshot.
3. Criar um catálogo de máquinas.

> **Nota:**
>
> Antes de criar um catálogo, certifique-se de ter um ou mais nós de cartucho HPE Moonshot e instale VDAs nesses nós. Você pode considerar o chassi HPE Moonshot como o hipervisor e os nós de cartucho como VMs.

4. Crie um grupo de entrega.
5. Migre o restante dos nós HPE Moonshot não gerenciados para o catálogo gerenciado ou grupo de entrega.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão no HPE Moonshot, consulte Conexão com o HPE Moonshot

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

## Ambientes de nuvem do Microsoft Azure Resource Manager

Ao usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™, familiarize-se com o seguinte:

- Azure Active Directory: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- Estrutura de consentimento: `<https://docs.microsoft.com/pt-br/azure/active-directory/manage-apps/plan-an-application-integration>`

- Entidade de serviço: `<https://docs.microsoft.com/pt-br/azure/active-directory/develop/app-objects-and-service-principals/>`

Para configurar seu Microsoft Azure Resource Manager, consulte Preparar para instalar.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes Azure, consulte Conexão com o Microsoft Azure

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas
- CTX219211: Configurar uma conta do Microsoft Azure Active Directory
- CTX219243: Conceder acesso do XenApp e XenDesktop à sua assinatura do Azure
- CTX219271: Implantar nuvem híbrida usando VPN site a site

## Ambientes do Microsoft System Center Configuration Manager

Sites que usam o Microsoft System Center Configuration Manager (Configuration Manager) para gerenciar o acesso a aplicativos e desktops podem estender esse uso para o Citrix Virtual Apps and Desktops™ usando estas opções:

- Instalar VDAs usando SCCM.
- **Recurso Wake Proxy do Configuration Manager:** O recurso Wake on LAN do Acesso Remoto a PC é compatível com o Configuration Manager. Para obter detalhes, consulte Wake on LAN - SCCM integrado.
- **Propriedades do Citrix Virtual Apps and Desktops:** Propriedades permitem identificar o Citrix Virtual Desktops™ para gerenciamento através do Configuration Manager. (Em algumas versões, o Configuration Manager usa o nome anterior do Citrix Virtual Apps and Desktops: XenApp e XenDesktop.)

### Propriedades

As propriedades estão disponíveis para o Microsoft System Center Configuration Manager para gerenciar desktops virtuais.

As propriedades booleanas exibidas no Configuration Manager aparecem como `1` ou `0`, não como true ou false.

As propriedades estão disponíveis para a classe `Citrix_virtualDesktopInfo` no namespace `Root\Citrix\DesktopInformation`. Os nomes das propriedades vêm do provedor Windows Management Instrumentation (WMI).

| PROPRIEDADE | DESCRIÇÃO |
|---|---|
| `AssignmentType` | Define o valor de IsAssigned. Os valores válidos são: `ClientIP`, `ClientName`, `None` e `User` (define `IsAssigned` como `True`) |
| `BrokerSiteName` | Retorna o mesmo valor que `HostIdentifier` |
| `DesktopCatalogName` | Catálogo de máquinas associado ao desktop. |
| `DesktopGroupName` | Grupo de entrega associado ao desktop. |
| `HostIdentifier` | Retorna o mesmo valor que `BrokerSiteName`. |
| `IsAssigned` | `True` para atribuir o desktop a um usuário, definido como `False` para um desktop aleatório |
| `IsMasterImage` | Permite decisões sobre o ambiente. Por exemplo, instalar aplicativos na imagem e não nas máquinas provisionadas. Os valores válidos são: `True` em uma VM que é usada como imagem. Este valor é definido durante a instalação com base em uma seleção, ou limpo em uma VM que é provisionada a partir dessa imagem. |
| `IsVirtualMachine` | `True` para uma máquina virtual, `false` para uma máquina física. |

| PROPRIEDADE | DESCRIÇÃO |
| --- | --- |
| `OSChangesPersist` | `False` se a imagem do sistema operacional do desktop for redefinida para um estado limpo toda vez que for reiniciada; caso contrário, `true`. |
| `PersistentDataLocation` | O local onde o Configuration Manager armazena dados persistentes. Isso não é acessível aos usuários. |
| `BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier` | Determinado quando o desktop se registra no Controller. Eles são nulos para um desktop que não foi totalmente registrado. |

Para coletar as propriedades, execute um inventário de hardware no Configuration Manager. Para visualizar as propriedades, use o Resource Explorer do Configuration Manager. Nestes casos, os nomes incluem espaços ou variam ligeiramente dos nomes das propriedades. Por exemplo, `BrokerSiteName` aparece como `Broker Site Name`.

- Configure o Configuration Manager para coletar propriedades WMI da Citrix do Citrix VDA
- Crie coleções de dispositivos baseadas em consulta usando propriedades WMI da Citrix
- Crie condições globais com base em propriedades WMI da Citrix
- Use condições globais para definir requisitos de tipo de implantação de aplicativo

Você também pode usar propriedades da Microsoft na classe Microsoft `CCM_DesktopMachine` no namespace `Root\ccm_vdi`. Para obter mais informações, consulte a documentação da Microsoft.

## Ambientes de virtualização Microsoft System Center Virtual Machine Manager

Siga esta orientação se você usa 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 diferentes versões do Hyper-V) não são suportados.

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

- VMs de SO de Desktop ou Servidor suportadas de Geração 1.
- VMs de SO de Desktop ou Servidor suportadas de Geração 2, incluindo suporte a Secure Boot.

### Instalar e configurar um hipervisor

> **Importante:**

> Todos os Delivery Controllers devem estar na mesma floresta que os servidores VMM.

1. Instale o servidor Microsoft Hyper-V e o VMM em seus servidores.
2. Instale o console do System Center Virtual Machine Manager em todos os Controllers. A versão do console deve corresponder à versão do servidor de gerenciamento. Embora um console anterior possa se conectar ao servidor de gerenciamento, o provisionamento de VDAs falha se as versões forem diferentes.
3. Verifique as seguintes informações da conta:

   A conta que você usa para especificar hosts no Studio é um administrador VMM ou administrador delegado VMM para as máquinas Hyper-V relevantes. Se esta conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados no Studio durante o processo de criação do host.

   A conta de usuário usada para a integração do Studio também deve ser membro do grupo de segurança local de administradores em cada servidor Hyper-V. Esta configuração suporta o gerenciamento do ciclo de vida da VM, como criação, atualização e exclusão de VM.

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

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

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

1. Em **Assistente para Criar Funções de Usuário**, selecione Administrador de Malha (Administrador Delegado) como uma função de usuário.
2. Em **Membros**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Escopo**, selecione os grupos de host aos quais você deseja que o administrador delegado tenha acesso.
4. Crie uma nova **Conta Executar como** usando as credenciais de usuário do administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

## Ambientes de virtualização Nutanix

Siga esta orientação ao usar o Nutanix Acropolis para fornecer máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™. O processo de configuração inclui as seguintes tarefas:

- Instale e registre o plug-in Nutanix em seu ambiente Citrix Virtual Apps and Desktops.
- Crie uma conexão com o hipervisor Nutanix Acropolis.
- Crie um catálogo de máquinas que usa um instantâneo de uma imagem mestre que você criou no hipervisor Nutanix.

Para obter mais informações, consulte o Guia de Instalação do plug-in MCS do Nutanix Acropolis, disponível no Portal de Suporte Nutanix.

### Instalar e registrar o plug-in Nutanix

Conclua o procedimento a seguir para instalar e registrar o plug-in Nutanix em todos os seus Delivery Controllers. Use o Citrix Studio para criar uma conexão com o Nutanix. Em seguida, crie um catálogo de máquinas que usa um instantâneo de uma imagem mestre que você criou no ambiente Nutanix.

> **Dica:**
>
> Recomendamos que você pare e reinicie o Citrix Host Service, o Citrix Broker Service e o Machine Creation Services™ ao instalar ou atualizar o plug-in Nutanix.

> Para obter informações sobre como instalar o plug-in Nutanix, consulte o site de Documentação Nutanix.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes Nutanix, consulte Conexão com Nutanix

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

## Soluções de nuvem e parceiros Nutanix

Citrix Virtual Apps and Desktops™ suporta a seguinte solução de nuvem e parceiro Nutanix:

- Clusters de Nuvem Nutanix no AWS

### Clusters de Nuvem Nutanix no AWS

O Citrix Virtual Apps and Desktops suporta Clusters de Nuvem Nutanix no AWS. Os clusters Nutanix simplificam a forma como os aplicativos são executados em nuvens privadas ou em várias nuvens públicas. Para obter mais informações sobre Clusters de Nuvem Nutanix no AWS, consulte Guia de Implantação e Usuário de Clusters de Nuvem Nutanix no AWS.

> **Dica:**
>
> Este suporte oferece a mesma funcionalidade que um cluster Nutanix local. Apenas um único cluster é suportado, o *Prism Element*. Para obter mais informações, consulte aqui.

### Requisitos

Você precisa do seguinte para usar Clusters Nutanix no AWS:

- Uma conta Nutanix.
- Uma conta AWS com as seguintes permissões:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

### Criar um Cluster Nutanix

Para criar um Cluster Nutanix:

1. Faça login na sua conta Nutanix.
2. Localize a opção **Nutanix cluster** e clique em **Launch**. O **Nutanix Console** é aberto. Para obter mais informações, consulte Introdução ao Nutanix Cluster no AWS.
3. Escolha criar uma **nova VPC**.

O processo de criação do cluster pode falhar com os seguintes erros:

- Falha ao criar o cluster dentro do tempo especificado. Excluindo cluster.
- Host Nutanix Cluster - Nó `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- Host Nutanix Cluster - Nó `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

Se o cluster falhou ao ser criado:

- Tente recriar um em uma região diferente.
- Certifique-se de excluir o Nutanix CloudFormation Stack (CFS) antes de tentar novamente.

Além de outros recursos, o Nutanix CFS cria:

- 1 VPC nomeada *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 sub-redes 10.0.128.0/24 e 10.0.129.0/24
- 1 gateway de Internet
- 1 gateway NAT

Assim que o cluster for criado, recupere o endereço do **Nutanix Prism**:

1. Vá para o **Nutanix Console**.
2. No canto superior direito do console, passe o mouse sobre o link **Launch Prism Element** e copie o URL.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão de soluções de nuvem e parceiros Nutanix, consulte Conexão com soluções de nuvem e parceiros Nutanix

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

## Ambientes de virtualização VMware

Siga esta orientação se você usa VMware para fornecer máquinas virtuais.

Instale o vCenter Server e as ferramentas de gerenciamento apropriadas. (Nenhum suporte é fornecido para a operação do vSphere vCenter Linked Mode.)

Se você planeja usar o MCS, não desative o recurso Datastore Browser no vCenter Server (descrito em `<https://kb.vmware.com/s/article/2101567>`). Ao desativar esse recurso, o MCS não funciona corretamente.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes VMware, consulte Conexão com VMware

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

# Soluções de nuvem e parceiros VMware

O Citrix Virtual Apps and Desktops™ oferece suporte às seguintes soluções de nuvem e parceiros VMware:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

## Integração do Azure VMware Solution (AVS)

O serviço Citrix Virtual Apps and Desktop oferece suporte a AVS. O AVS fornece infraestrutura de nuvem contendo clusters vSphere criados pela infraestrutura do Azure. Aproveite o serviço Citrix Virtual Apps and Desktop para usar o AVS para provisionar sua carga de trabalho VDA da mesma forma que você usaria o vSphere em ambientes locais.

### Configurar o cluster AVS

Para habilitar o Citrix Virtual Apps™ and Desktop Service a usar o AVS, execute as seguintes etapas no Azure:

- Solicitar uma cota de host
- Registrar o provedor de recursos Microsoft.AVS
- Lista de Verificação de Rede
- Criar uma nuvem privada do Azure VMware Solution
- Acessar uma nuvem privada do Azure VMware Solution
- Configurar a rede para sua nuvem privada VMware no Azure
- Configurar DHCP para Azure VMware Solution
- Adicionar um segmento de rede no Azure VMware Solution
- Verificar o ambiente do Azure VMware Solution

#### SOLICITAR COTA DE HOST PARA CLIENTES DO AZURE ENTERPRISE AGREEMENT

Na página **Ajuda + Suporte** do portal do Azure, selecione **Nova solicitação de suporte** e inclua as seguintes informações:

- Tipo de problema: Técnico
- Assinatura: Selecione sua assinatura
- Serviço: Todos os serviços > Azure VMware Solution
- Recurso: Pergunta geral

- Resumo: Necessidade de capacidade
- Tipo de problema: Problemas de gerenciamento de capacidade
- Subtipo de problema: Solicitação do cliente para cota/capacidade de host adicional

Na **Descrição** do tíquete de suporte, inclua as seguintes informações na guia **Detalhes**:

- POC ou Produção
- Nome da Região
- Número de hosts
- Quaisquer outros detalhes

> **Nota:**
>
> O AVS requer um mínimo de três hosts e recomenda que você use redundância de N+1 hosts.

> Após especificar os detalhes para o tíquete de suporte, selecione **Revisar + Criar** para enviar a solicitação ao Azure.

### REGISTRAR O PROVEDOR DE RECURSOS MICROSOFT.AVS

Após solicitar a cota de host, registre o provedor de recursos:

1. Faça login no portal do Azure.
2. No menu do portal do Azure, selecione **Todos os serviços**.
3. No menu **Todos os serviços**, insira a assinatura e selecione **Assinaturas**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Provedores de recursos** e insira **Microsoft.AVS** na barra de pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

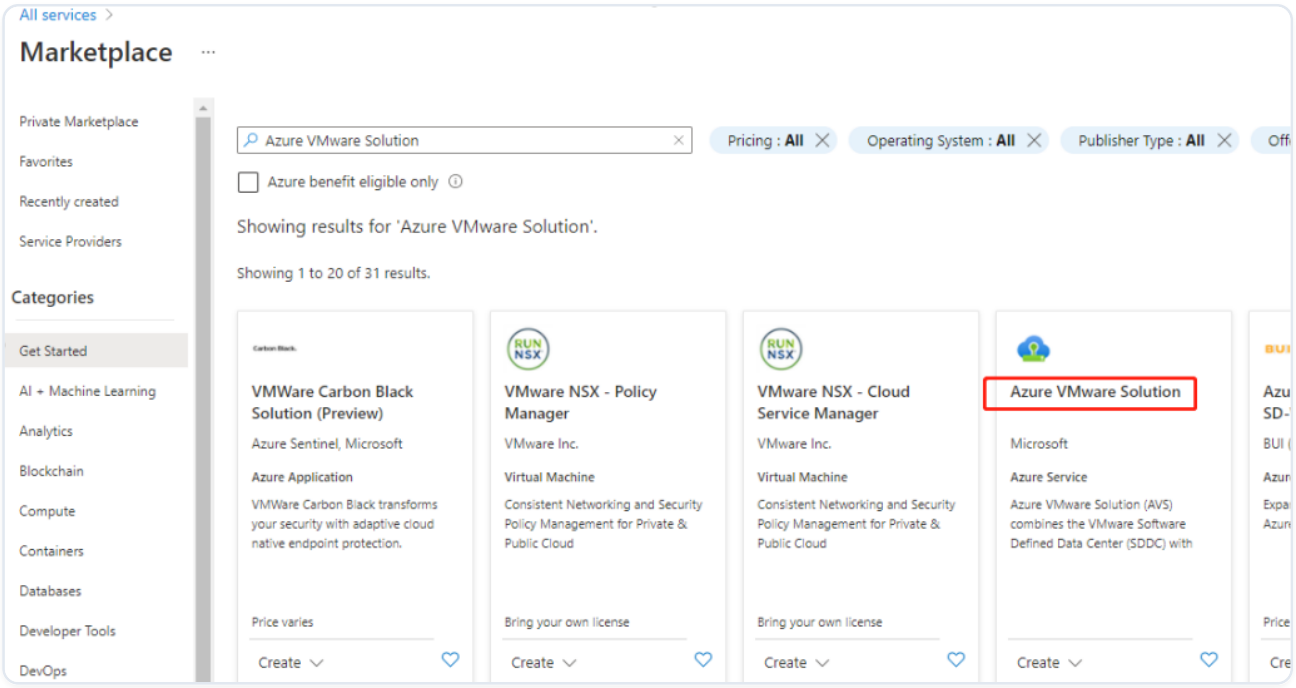
### CONSIDERAÇÕES SOBRE REDE

O AVS oferece serviços de rede que exigem intervalos de endereços de rede específicos e portas de firewall. Consulte Lista de verificação de planejamento de rede para a Solução VMware do Azure para obter mais informações.

### CRIAR UMA NUVEM PRIVADA DO AZURE VMWARE SOLUTION

Após considerar os requisitos de rede para seu ambiente, crie uma nuvem privada ASV:

1. Faça login no portal do Azure.
2. Selecione **Criar um novo recurso**.
3. Na caixa de texto **Pesquisar no Marketplace**, digite *Azure VMware Solution* e selecione **Azure VMware Solution** na lista.



imagem

Na janela **Azure VMware Solution**:

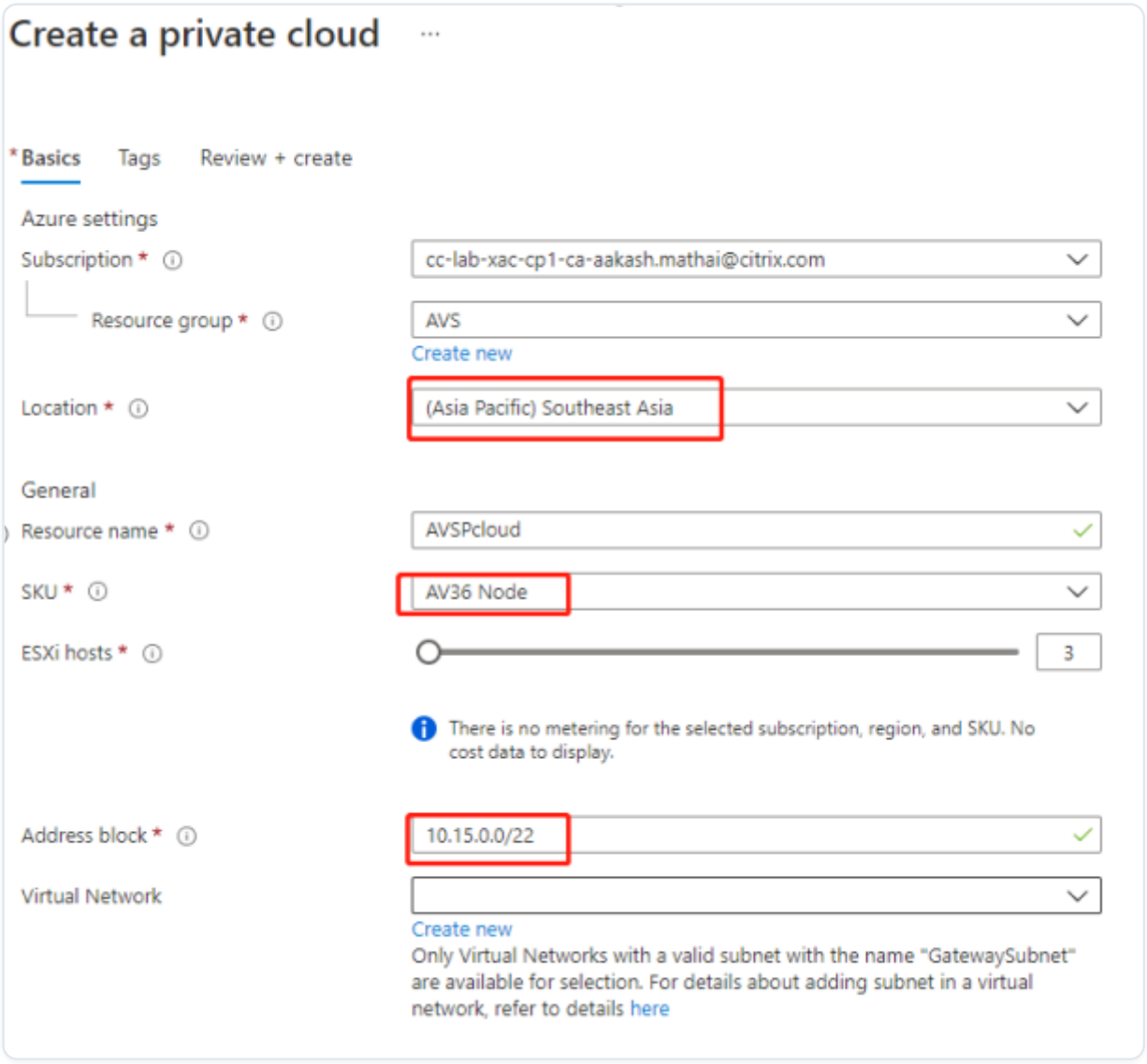
1. Selecione **Criar**.
2. Clique na guia **Básico**.
3. Insira os valores para os campos, usando as informações na tabela abaixo:

| CAMPO | VALOR |
|---|---|
| Assinatura | Selecione a assinatura que você planeja usar para a implantação. Todos os recursos em uma assinatura do Azure são cobrados juntos. |
| Grupo de recursos | Selecione o grupo de recursos para sua nuvem privada. Um grupo de recursos do Azure é um contêiner lógico no qual os recursos do Azure são implantados e gerenciados. Alternativamente, você pode criar um novo grupo de recursos para sua nuvem privada. |

| CAMPO | VALOR |
|---|---|
| Localização | Selecione um local, como leste dos EUA. Esta é a região que você definiu durante a fase de planejamento. |
| Nome do recurso | Forneça o nome da sua nuvem privada do Azure VMware Solution. |
| SKU | Selecione AV36. |
| Hosts | Mostra o número de hosts alocados para o cluster da nuvem privada. O valor padrão é 3, que pode ser aumentado ou diminuído após a implantação. |
| Bloco de endereços | Forneça um bloco de endereços IP para a nuvem privada. O CIDR representa a rede de gerenciamento da nuvem privada e será usado para os serviços de gerenciamento do cluster, como vCenter Server e NSX-T Manager. Use o espaço de endereço /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure, bem como a redes locais. |
| Rede Virtual | Deixe este campo em branco porque o circuito ExpressRoute do Azure VMware Solution é estabelecido como uma etapa pós-implantação. |

Na tela **Criar uma nuvem privada**:

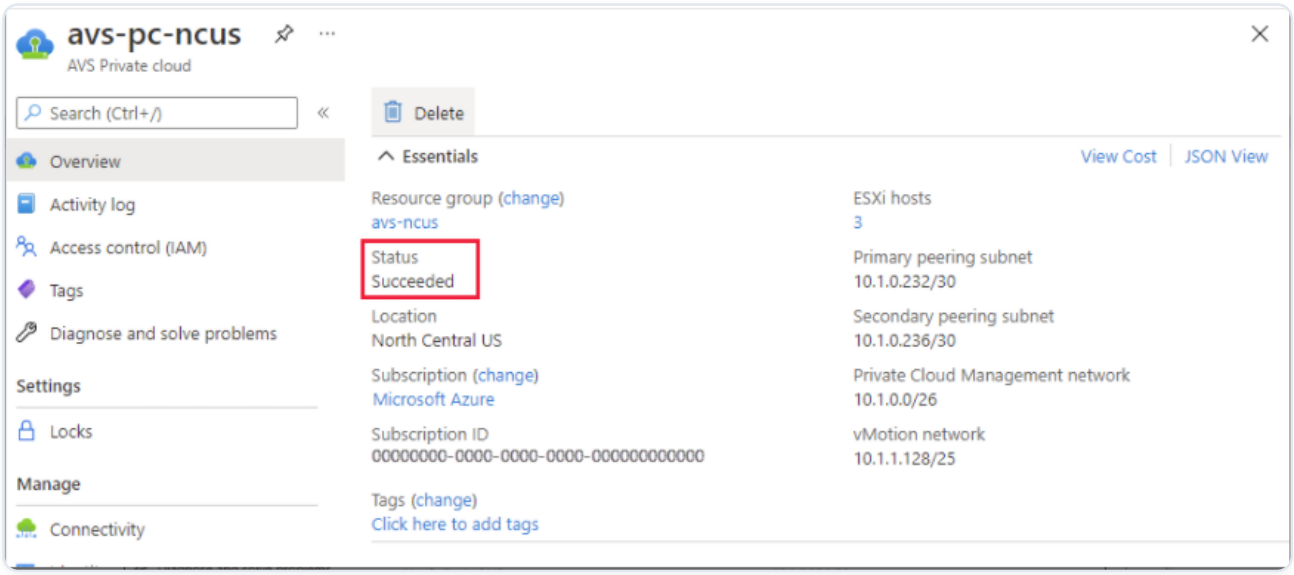
1. No campo **Localização**, selecione a região que possui o AVS; a região do grupo de recursos é a mesma da região do AVS.
2. No campo **SKU**, selecione **Nó AV36**.
3. Especifique um endereço IP no campo **Bloco de Endereços**. Por exemplo, 10.15.0.0/22.
4. Selecione **Revisar + Criar**.
5. Após revisar as informações, clique em **Criar**.




**Dica:**

A criação de uma nuvem privada pode levar de 3 a 4 horas. Adicionar um único host ao cluster pode levar de 30 a 45 minutos.

Verifique se a implantação foi bem-sucedida. navegar para o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Succeeded**, a implantação estará concluída.




### ACESSAR UMA NUVEM PRIVADA DO AZURE VMWARE SOLUTION

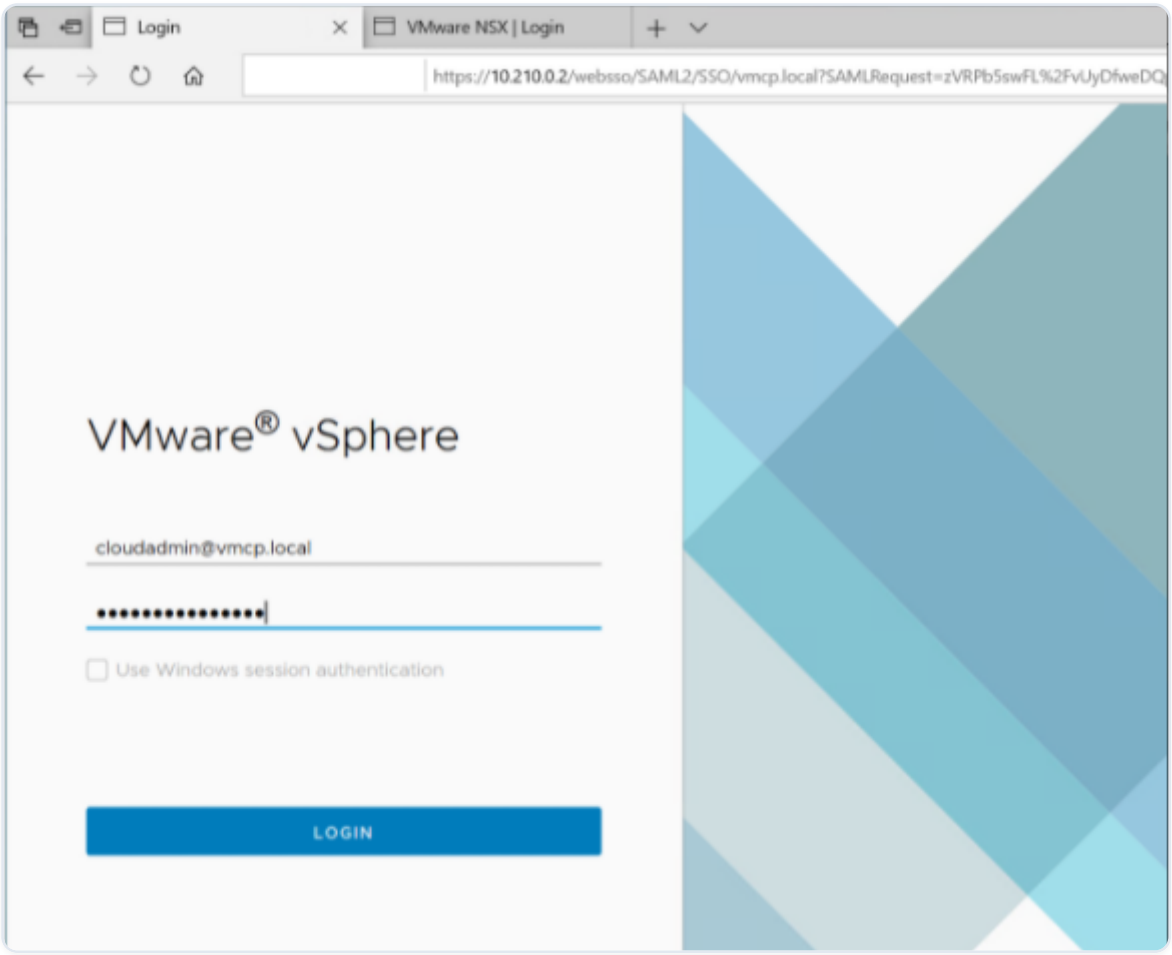
Depois de criar uma nuvem privada, crie uma VM Windows e conecte-se ao vCenter local da sua nuvem privada.

Criar uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar** e, em seguida, pesquise e selecione **Microsoft Windows 10/2016/2019**.
2. Clique em **Criar**.
3. Insira as informações necessárias e selecione **Revisar + Criar**.
4. Assim que a validação for aprovada, selecione **Criar** para iniciar o processo de criação da máquina virtual.

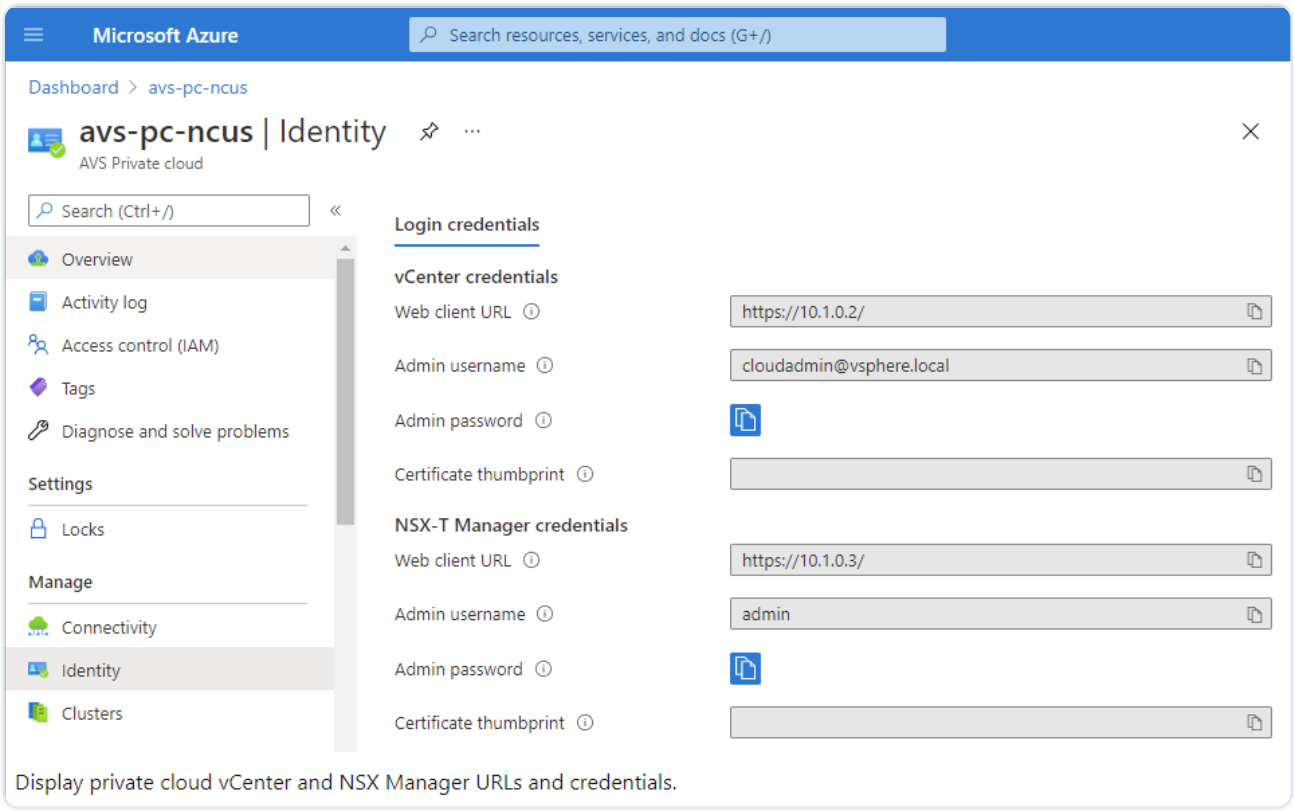
Conectar-se ao vCenter local da sua nuvem privada

1. Faça login no **vSphere Client com VMware vCenter SSO** como administrador de nuvem.




2. No portal do Azure, selecione sua nuvem privada e, em seguida, **Gerenciar > Identidade**.

As URLs e as credenciais de usuário para o vCenter da nuvem privada e o NSX-T Manager aparecem:




Após confirmar as URLs e as credenciais de usuário:

1. navegar para a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegar para as URLs do vCenter e do NSX-T Manager em duas abas do navegador. Na aba do vCenter, insira as credenciais de usuário *cloudadmin@vmcp.local* da etapa anterior.

### CONFIGURAR A REDE PARA SUA NUVEM PRIVADA VMWARE NO AZURE

Após acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.
Criar uma rede virtual

1. Faça login no portal do Azure.
2. navegar para o grupo de recursos criado anteriormente.
3. Selecione **+ Adicionar** para definir um novo recurso.
4. Na caixa de texto **Pesquisar no Marketplace**, digite *rede virtual*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Rede Virtual**, selecione **Criar** para configurar a rede virtual para sua nuvem privada.
6. Na página **Criar Rede Virtual**, insira os detalhes da sua rede virtual.
7. Na guia **Básico**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Avançar: Endereços IP.**

8. Na guia **Endereços IP**, em espaço de endereço IPv4, insira o endereço criado anteriormente.

> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço que você usou ao criar sua nuvem privada.

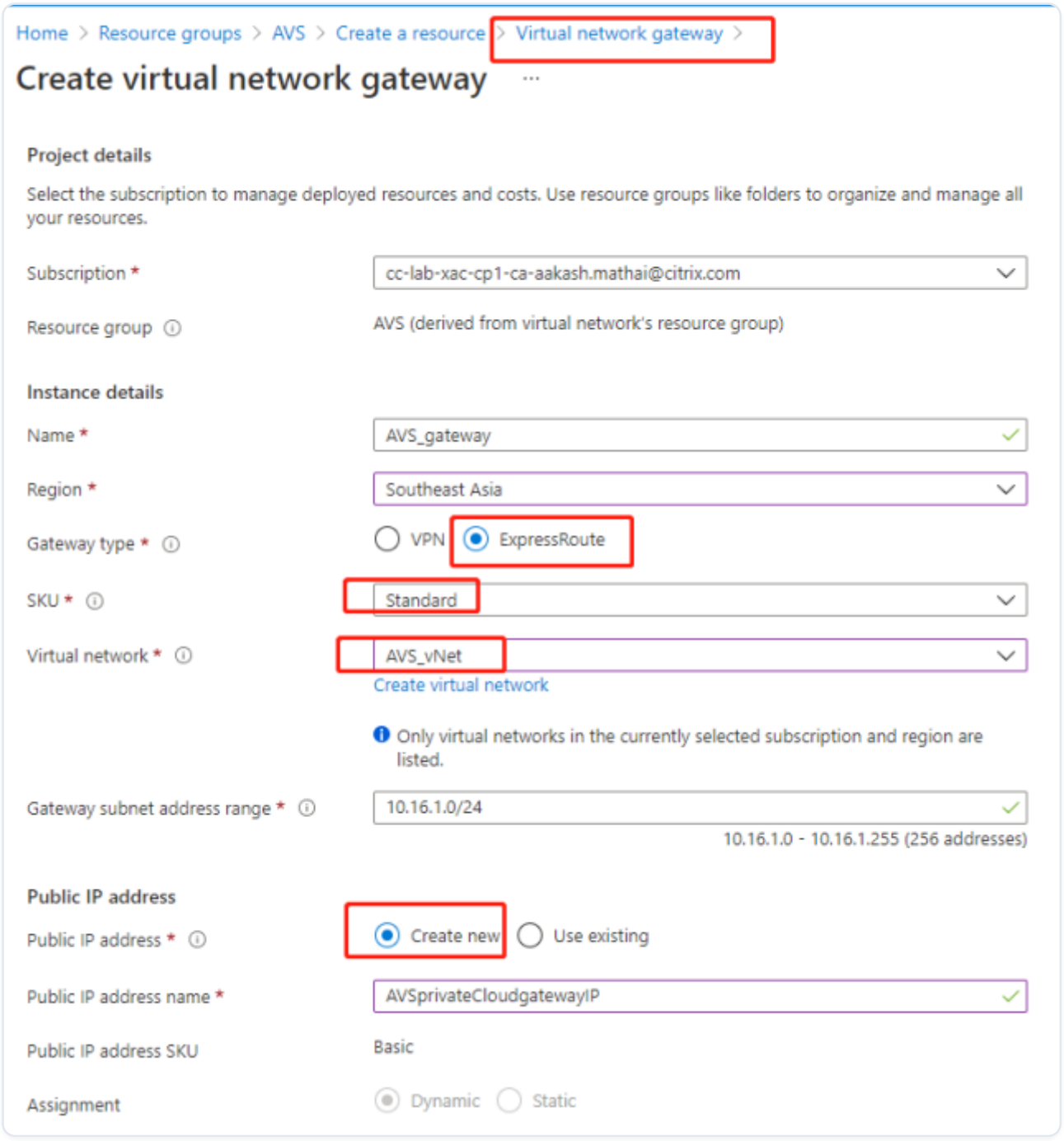
> Após inserir o espaço de endereço:

1. Selecione **+ Adicionar sub-rede**.
2. Na página **Adicionar sub-rede**, dê um nome à sub-rede e um intervalo de endereços apropriado.
3. Clique em **Adicionar.**
4. Selecione **Revisar + criar**.
5. Verifique as informações e clique em **Criar**. Assim que a implantação for concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual

Após criar uma rede virtual, crie um gateway de rede virtual.

1. No seu grupo de recursos, selecione **+ Adicionar** para adicionar um novo recurso.
2. Na caixa de texto **Pesquisar no Marketplace**, digite *gateway de rede virtual*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Gateway de Rede Virtual**, clique em **Criar**.
4. Na guia **Básico** da página **Criar gateway de rede virtual**, forneça valores para os campos.
5. Clique em **Revisar + criar**.



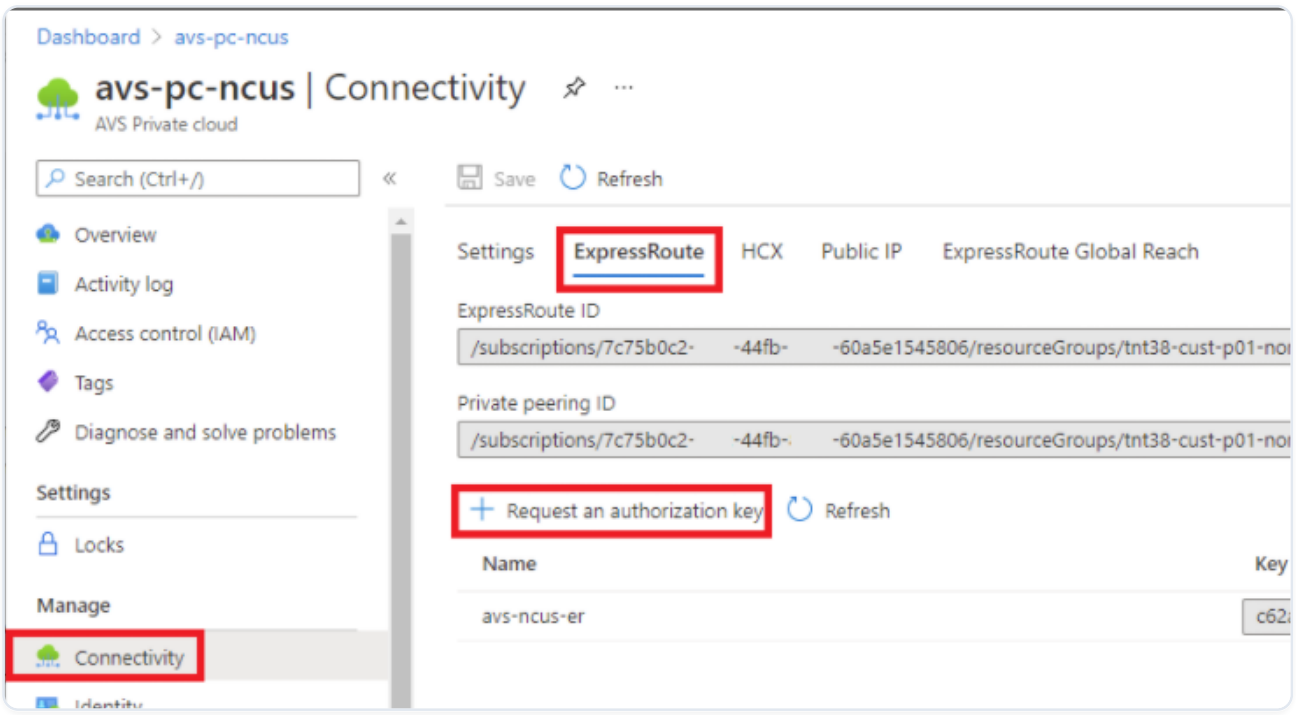

Após revisar a configuração do gateway de rede virtual, clique em **Criar** para implantar seu gateway de rede virtual. Assim que a implantação for concluída, conecte sua conexão **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada Azure AVS.

### CONECTAR O EXPRESSROUTE AO GATEWAY DE REDE VIRTUAL

Após implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada do Azure AVS:

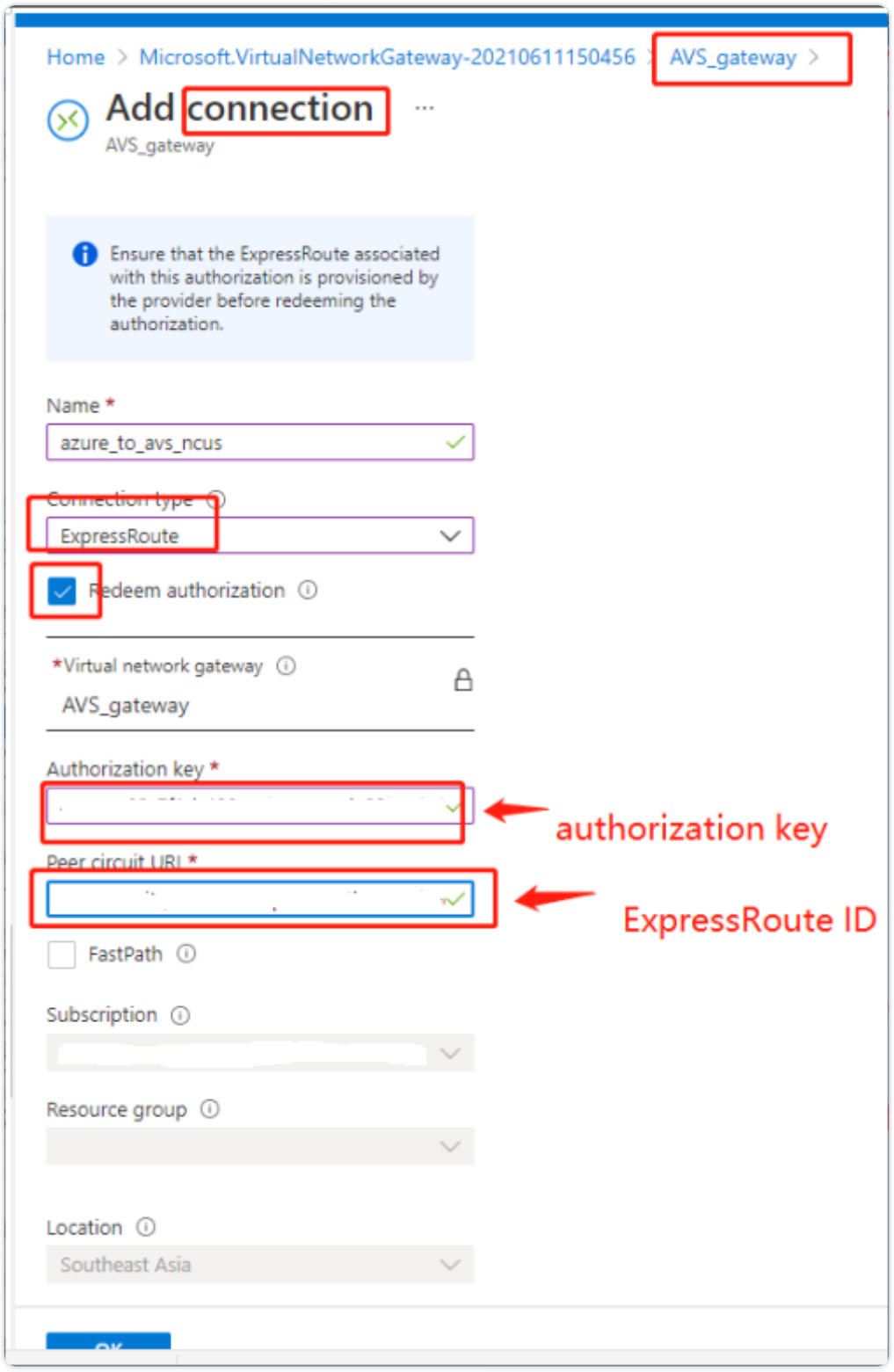
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegar até a **nuvem privada da Solução VMware do Azure**. Selecione **Gerenciar > Conectividade > ExpressRoute** e, em seguida, selecione **+ Solicitar uma chave de autorização.**

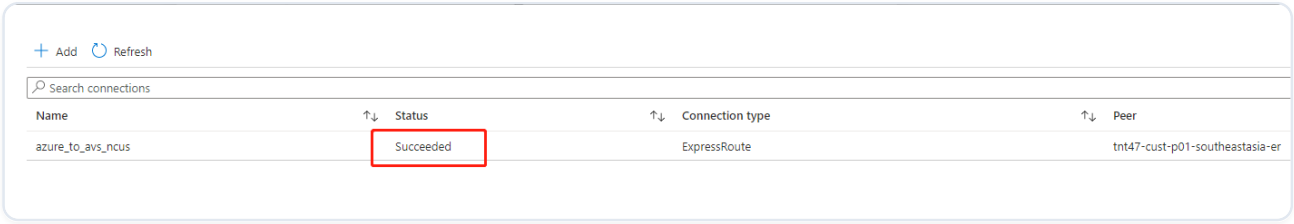



Após solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Criar**. Pode levar cerca de 30 segundos para criar a chave. Uma vez criada, a nova chave aparece na lista de chaves de autorização para a nuvem privada.
2. Copie a **chave de autorização** e o **ID do ExpressRoute**. Você precisará deles para concluir o processo de emparelhamento. A chave de autorização desaparece depois de algum tempo, então copie-a assim que aparecer.
3. navegar até o **gateway de rede virtual** que você planeja usar e selecione **Conexões > + Adicionar**.
4. Na página **Adicionar conexão**, forneça valores para os campos e selecione **OK.**




A conexão é estabelecida entre o seu circuito ExpressRoute e a sua rede virtual:



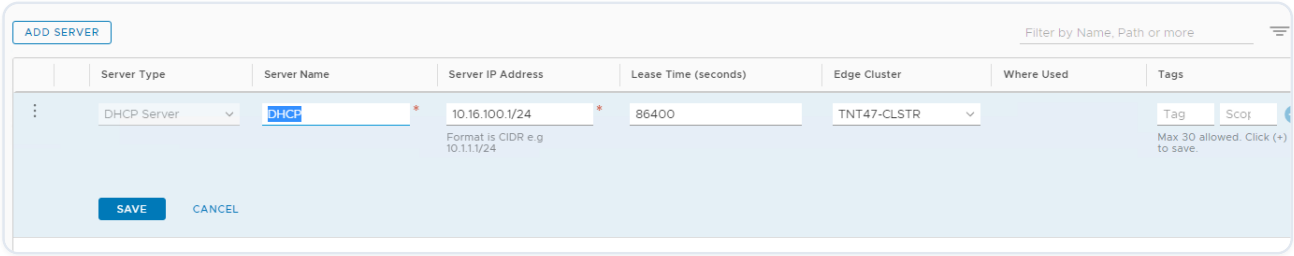
### CONFIGURAR DHCP PARA AZURE VMWARE SOLUTION

Após conectar o ExpressRoute ao gateway virtual, configure o DHCP.

Use o NSX-T para hospedar seu servidor DHCP

No NSX-T Manager:

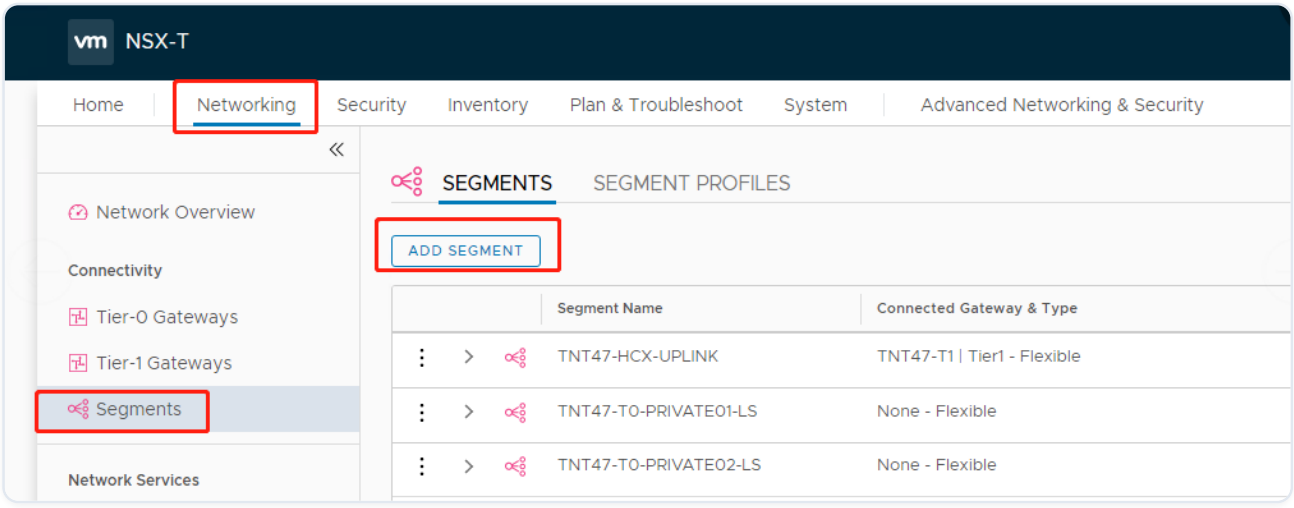
1. Selecione **Rede > DHCP** e então selecione **Adicionar Servidor**.
2. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Gateways de Camada 1**, selecione as reticências verticais no gateway de Camada 1 e então selecione **Editar**.
5. Selecione **Nenhum Conjunto de Alocação de IP** para adicionar uma sub-rede.
6. Selecione **Servidor DHCP Local** para o **Tipo**.
7. Para o **Servidor DHCP**, selecione **DHCP Padrão** e então clique em **Salvar**.
8. Clique em **Salvar** novamente e, em seguida, selecione **Fechar Edição**.




### ADICIONAR UM SEGMENTO DE REDE NO AZURE VMWARE SOLUTION

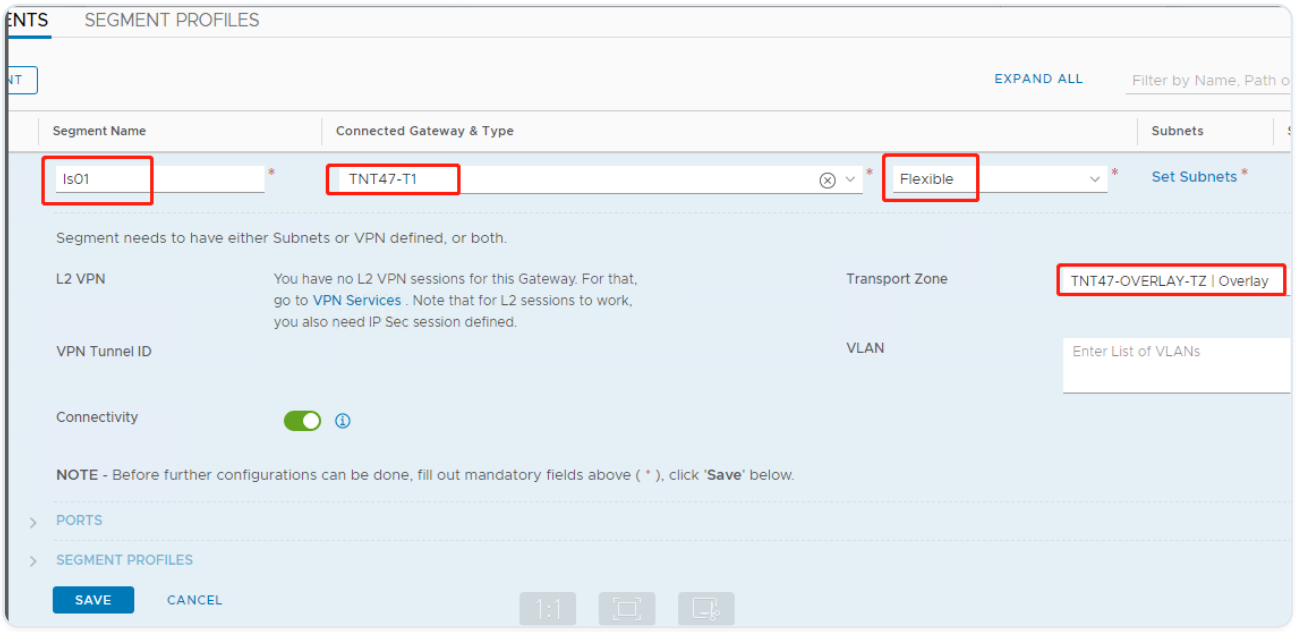
Após configurar o DHCP, adicione um segmento de rede.

Para adicionar um segmento de rede, no NSX-T Manager, selecione **Rede > Segmentos** e, em seguida, clique em **Adicionar Segmento**.




Na tela **Perfil de segmentos**:

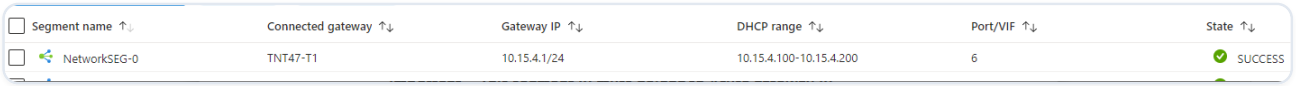
1. Insira um **nome** para o segmento.
2. Selecione o **Gateway Tier-1 (TNTxx-T1)** como o **Gateway Conectado** e deixe o **Tipo** como **Flexível**.
3. Selecione a **Zona de Transporte (TNTxx-OVERLAY-TZ)** de sobreposição pré-configurada.
4. Clique em **Definir Sub-redes**.



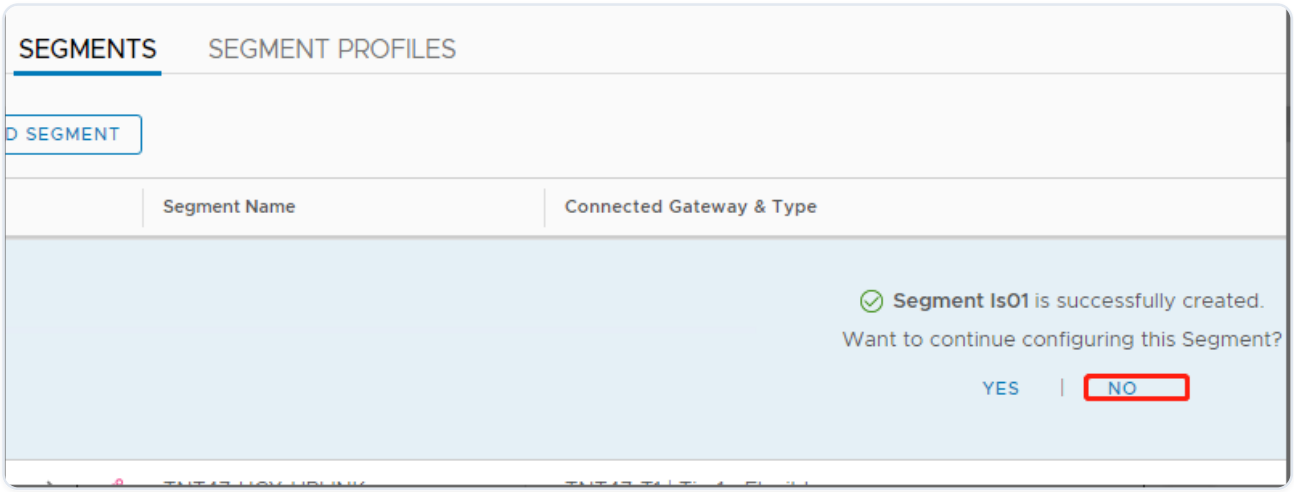

Na seção **Sub-redes**:

1. Insira o endereço IP do gateway.
2. Selecione **Adicionar**.

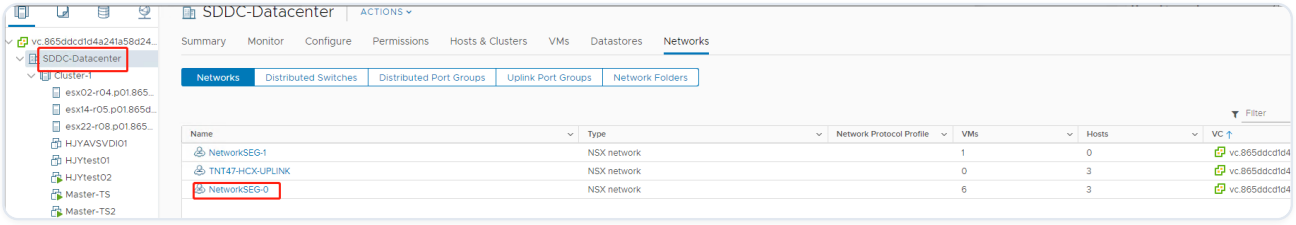
> **Importante:**
>
> Este endereço IP de segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.
>
> O intervalo DHCP deve pertencer ao endereço IP do segmento:




Selecione **Não** para recusar a opção de continuar configurando o segmento:

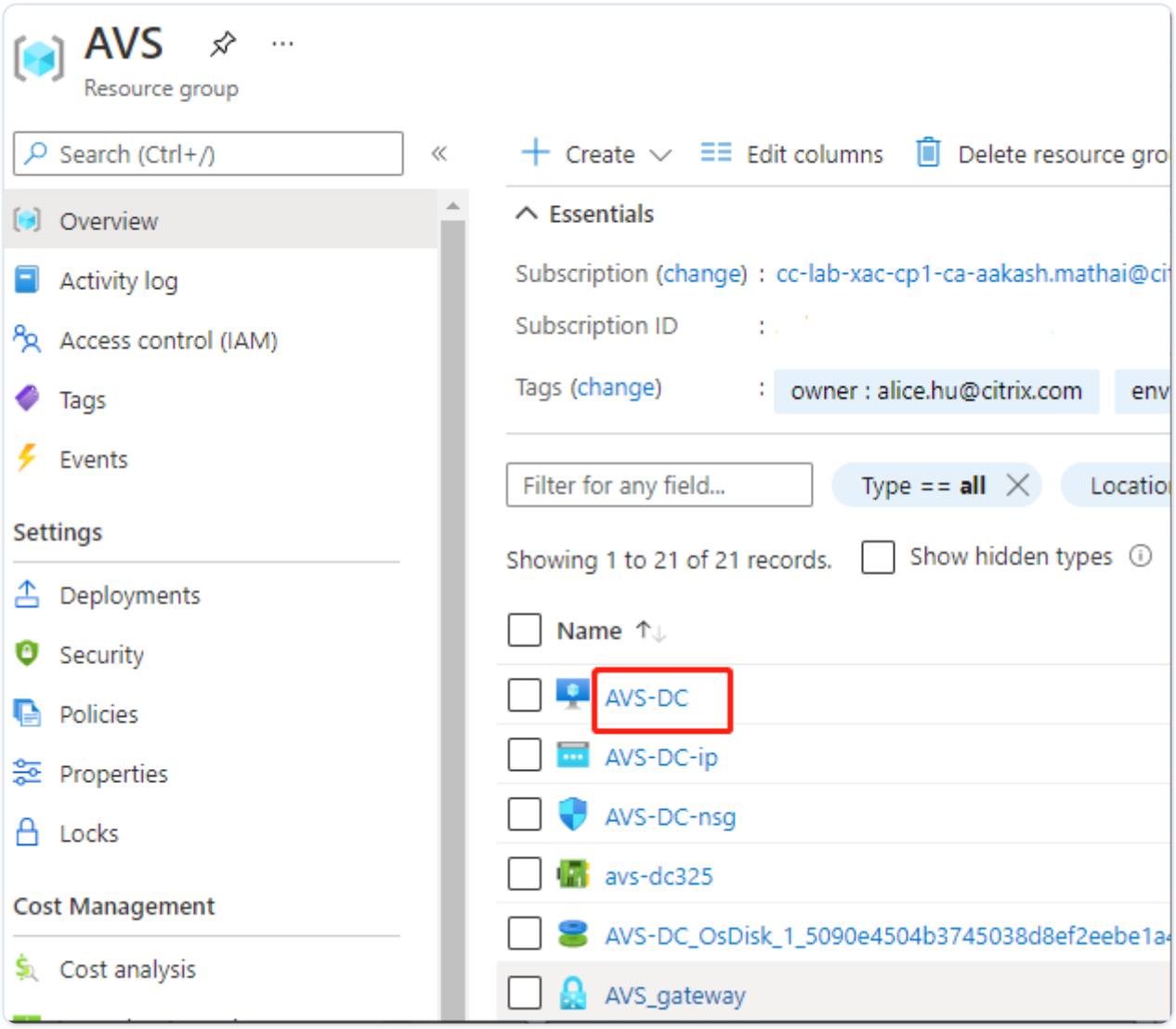



No vCenter, selecione **Networking > SDDC-Datacenter**:

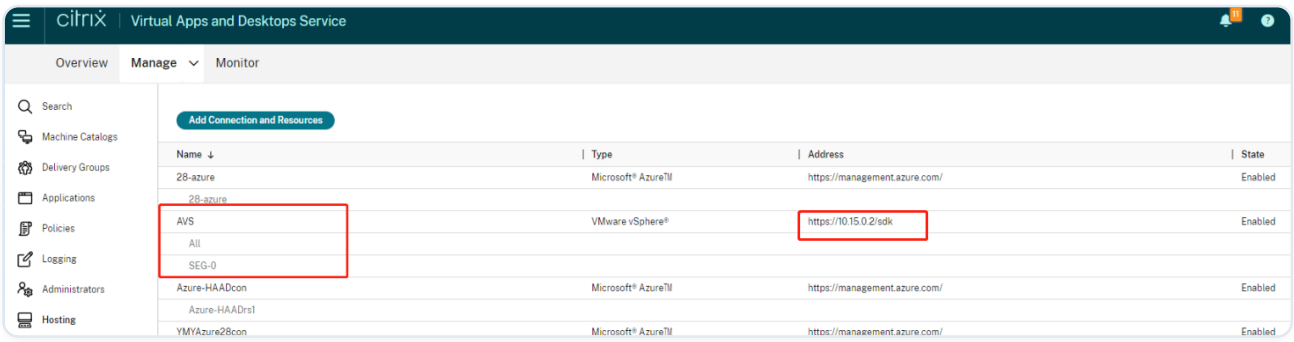



## VERIFICAR O AMBIENTE AZURE AVS

Configure uma conexão direta e um conector no grupo de recursos do Azure:




Verifique a conexão com as credenciais do vCenter:




## Google Cloud VMware Engine

O Citrix Virtual Apps and Desktops permite migrar cargas de trabalho Citrix locais baseadas em VMware para o Google Cloud VMware Engine.

### Configurar o Google Cloud VMware Engine

O procedimento a seguir descreve como adquirir e configurar um cluster no Google Cloud VMware Engine.

### ACESSAR O PORTAL DO VMWARE ENGINE

1. No **Google Cloud Console**, clique no menu de navegação.
2. Na seção **Compute**, clique em **VMware Engine** para abrir o VMware Engine em uma nova guia do navegador.

### REQUISITOS PARA CRIAR A PRIMEIRA NUVEM PRIVADA

Você deve ter acesso ao Google Cloud VMware Engine, cota de nó do VMware Engine disponível e uma função IAM apropriada. Prepare os seguintes requisitos antes de continuar a criar sua nuvem privada:

1. Solicite acesso à API e cota de nó. Para obter mais informações, consulte Solicitando acesso à API e cota.
2. Anote os intervalos de endereço que você deseja usar para os dispositivos de gerenciamento VMware e a rede de implantação HCX. Para obter mais informações, consulte Requisitos de rede.
3. Obtenha a função IAM de Administrador de Serviço do VMware Engine.

### CRIE SUA PRIMEIRA NUVEM PRIVADA

1. Acesse o portal do VMware Engine.
2. Na página inicial do VMware Engine, clique em **Criar uma nuvem privada**. O local de hospedagem e os tipos de nó de hardware são listados.
3. Selecione o número de nós para a nuvem privada. Pelo menos três nós são necessários.
4. Insira um intervalo de Roteamento Entre Domínios Sem Classe (CIDR) para a rede de gerenciamento VMware.
5. Insira um intervalo CIDR para a rede de implantação HCX.

> **Importante:**
>
> O intervalo CIDR não deve se sobrepor a nenhuma de suas sub-redes locais ou da nuvem. O intervalo CIDR deve ser /27 ou superior.

6. Selecione **Revisar e criar**.
7. Revise as configurações. Para alterar qualquer configuração, clique em **Voltar**.
8. Clique em **Criar** para começar a criar a nuvem privada.

À medida que o VMware Engine cria sua nova nuvem privada, ele implanta vários componentes VMware e configura políticas iniciais de Autoscale™ para clusters na nuvem privada. A criação da nuvem privada pode levar de 30 minutos a 2 horas. Após a conclusão do provisionamento, você receberá um e-mail.

### CONFIGURAR O GATEWAY VPN DO GOOGLE CLOUD VMWARE ENGINE

Para estabelecer uma conectividade inicial com o Google Cloud VMware Engine, você pode usar um gateway VPN. Este é um VPN de cliente baseado em OpenVPN, através do qual você pode se conectar ao seu vCenter do VMware Software Defined Data Center (SDDC) e realizar qualquer configuração inicial necessária.

Antes de implantar o gateway VPN, configure o intervalo de **Edge Services** para a região onde seu SDDC está implantado. Para fazer isso:

1. Faça login no portal **Google Cloud VMware Engine** e vá para **Rede > Configurações Regionais**. Clique em **Adicionar Região**.
2. Escolha a região onde seu SDDC está implantado e habilite **Acesso à Internet** e **Serviço de IP Público**.
3. Forneça o intervalo de Serviços de Borda anotado durante o planejamento e clique em **Enviar**. A habilitação desses serviços leva de 10 a 15 minutos.

   Uma vez concluído, os Serviços de Borda aparecem como **Habilitados** na página Configurações Regionais. A habilitação dessas configurações permite que IPs Públicos sejam alocados ao seu SDDC, o que é um requisito para implantar um gateway VPN.

Para implantar um gateway VPN:

1. No portal **Google Cloud VMware Engine**, vá para **Rede > Gateways VPN**. Clique em **Criar Novo Gateway VPN**.
2. Forneça o nome para o gateway VPN e a sub-rede do cliente reservada durante o planejamento. Clique em **Avançar**.
3. Selecione os usuários para conceder acesso VPN. Clique em **Avançar**.
4. Especifique as redes que devem ser acessíveis via VPN. Clique em **Avançar**.
5. Uma tela de resumo é exibida. Verifique as seleções e clique em **Enviar** para criar o Gateway VPN. A página Gateways VPN é exibida com o status do novo gateway VPN como **Criando**.
6. Depois que o status mudar para **Operacional**, clique no novo gateway VPN.
7. Clique em **Baixar minha configuração VPN** para baixar um arquivo ZIP contendo perfis OpenVPN pré-configurados para o gateway VPN. Perfis para conexão via UDP/1194 e TCP/

443 estão disponíveis. Escolha sua preferência e importe-a para o Open VPN e, em seguida, conecte-se.

8. Vá para **Recursos** e selecione seu SDDC.

### CONECTAR A VPN

1. Estabeleça uma conexão ponto a site entre sua rede local e a nuvem privada por meio da configuração do Gateway VPN. Consulte Configurar o Gateway VPN do Google Cloud VMware Engine.
2. Carregue a configuração VPN baixada em Configurar o Gateway VPN do Google Cloud VMware Engine.
3. Importe para seu cliente VPN, por exemplo, OpenVPN Connect.

Para obter mais informações, consulte Conectando usando VPN.

### CRIAR PRIMEIRA SUB-REDE

Acessar o NSX-T Manager no portal do VMware Engine
O processo de criação de uma sub-rede ocorre no NSX-T, que você acessa através do VMware Engine. Faça o seguinte para acessar o NSX-T Manager.

1. Faça logon no portal **Google Cloud VMware Engine**.
2. Na navegação principal, vá para **Recursos**.
3. Clique no **nome da nuvem privada** correspondente à nuvem privada onde você deseja criar a sub-rede.
4. Na página de detalhes da sua nuvem privada, clique na guia **vSphere Management Network**.
5. Clique no **FQDN** correspondente ao NSX-T Manager.
6. Quando solicitado, insira suas credenciais de login. Se você configurou o vIDM e o conectou a uma fonte de identidade, como o Active Directory, use suas credenciais de fonte de identidade.

> **Lembrete:**
>
> Você pode recuperar as credenciais geradas na página de detalhes da nuvem privada.

Configurar o serviço DHCP para a sub-rede
Antes de criar uma sub-rede, configure um serviço DHCP:

No NSX-T Manager:

1. Vá para **Rede > DHCP**. O painel de rede mostra que o serviço DHCP cria um gateway Tier-0 e um gateway Tier-1.
2. Para começar a provisionar um servidor DHCP, clique em **Adicionar Servidor**.
3. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
4. Clique em **Salvar** para criar o serviço DHCP.

Faça o seguinte para anexar este serviço DHCP ao gateway Tier-1 relevante. Um gateway Tier-1 padrão já é provisionado pelo serviço DHCP:

1. Selecione **Gateways Tier 1**, selecione as reticências verticais no gateway Tier-1 e, em seguida, selecione **Editar**.
2. No campo **Gerenciamento de Endereços IP**, selecione **Nenhum Conjunto de Alocação de IP**.
3. Selecione **Servidor DHCP Local** para o **Tipo**.
4. Selecione o servidor DHCP que você criou para o **Servidor DHCP**.
5. Clique em **Salvar**.
6. Clique em **Fechar Edição**.

Agora você pode criar um segmento de rede no NSX-T. Para obter mais informações sobre DHCP no NSX-T, consulte a documentação da VMware para DHCP.

Criar um segmento de rede no NSX-T

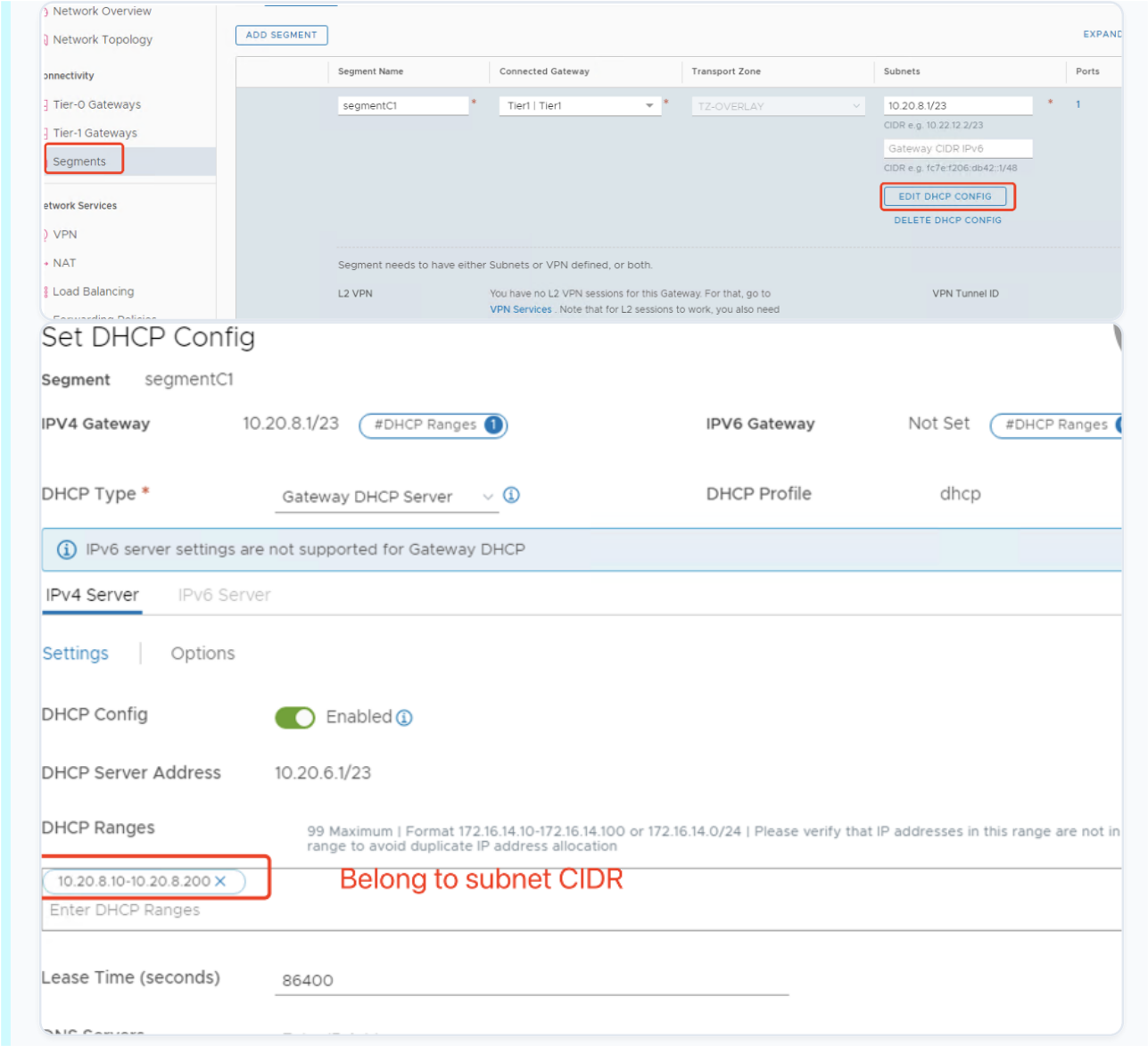
Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede NSX-T para sua nuvem privada:

1. No NSX-T Manager, vá para **Rede > Segmentos**.
2. Clique em **Adicionar Segmento**.
3. Insira um nome para o segmento.
4. Selecione o **Tier-1** como o **Gateway Conectado** e deixe o Tipo como **Flexível**.
5. Clique em **Definir Sub-redes**.
6. Clique em **Adicionar Sub-redes**.
7. Insira o intervalo da sub-rede em **Gateway IP/Prefix Length**. Especifique o intervalo da sub-rede com **.1** como o último octeto. Por exemplo, **10.12.2.1/24**.
8. Especifique os intervalos DHCP e clique em **ADD**.
9. Em **Transport Zone**, selecione **TZ-OVERLAY** na lista suspensa.

10. Clique em **Salvar**. Agora você pode selecionar este segmento de rede no vCenter ao criar uma VM.

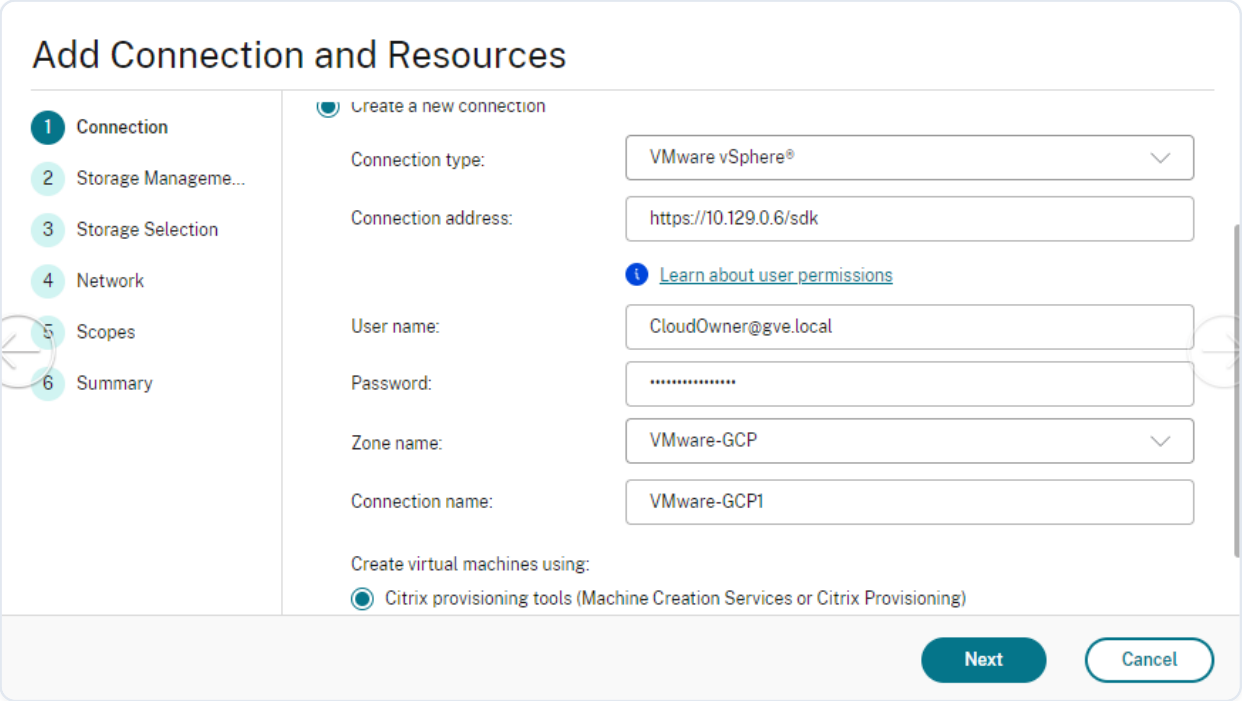
Em uma determinada região, você pode configurar no máximo 100 rotas exclusivas do VMware Engine para sua rede VPC usando acesso a serviços privados. Isso inclui, por exemplo, intervalos de endereços IP de gerenciamento de nuvem privada, segmentos de rede de carga de trabalho NSX-T e intervalos de endereços IP de rede HCX. Este limite inclui todas as nuvens privadas na região.

> **Nota:**
>
> Há um problema de configuração do Google Cloud devido ao qual você precisa configurar a definição do intervalo DHCP várias vezes. Portanto, certifique-se de configurar a definição do intervalo DHCP após a configuração do Google Cloud. Clique em **EDIT DHCP CONFIG** para configurar os intervalos DHCP.




## CRIAR A CONEXÃO GOOGLE CLOUD VMWARE NO CITRIX STUDIO

1. Crie uma máquina no vCenter.
2. Inicie o Citrix Studio.
3. Selecione o nó de hospedagem e clique em **Adicionar Conexão e Recursos**.
4. Na tela **Conexão**, selecione **Criar uma nova Conexão** e os seguintes detalhes:




a. Selecione **Tipo de conexão** como **VMware vSphere**.

b. No **Endereço de conexão**, insira o endereço IP privado do vCenter.

c. Insira as credenciais do vCenter.

d. Insira um nome de conexão.

e. Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Rede**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

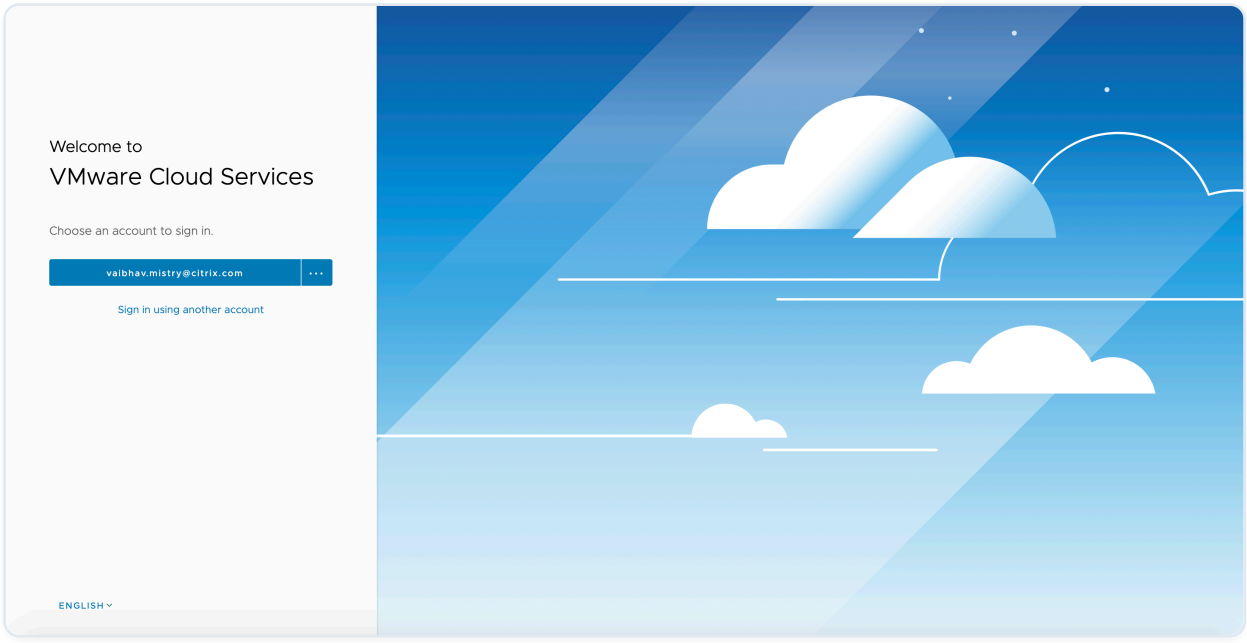
## VMware Cloud no Amazon Web Services (AWS)

O VMware Cloud on Amazon Web Services (AWS) permite migrar cargas de trabalho Citrix locais baseadas em VMware para a AWS Cloud.

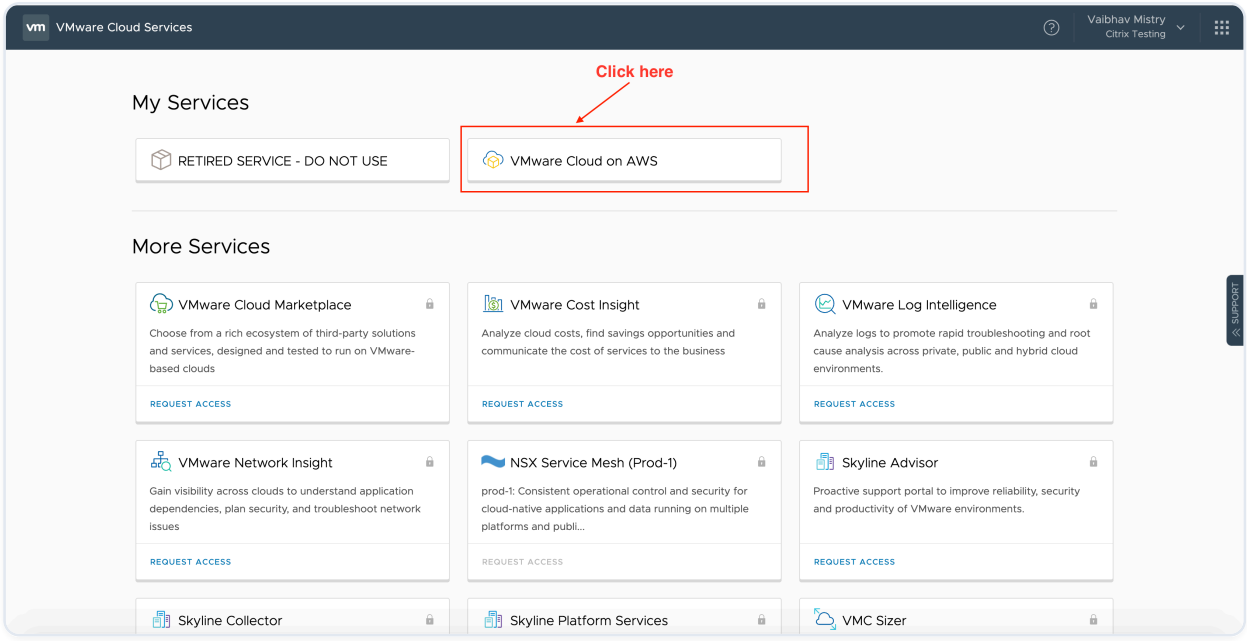
Este artigo descreve o procedimento para configurar um VMware Cloud no AWS.

### Acessar o ambiente VMware Cloud

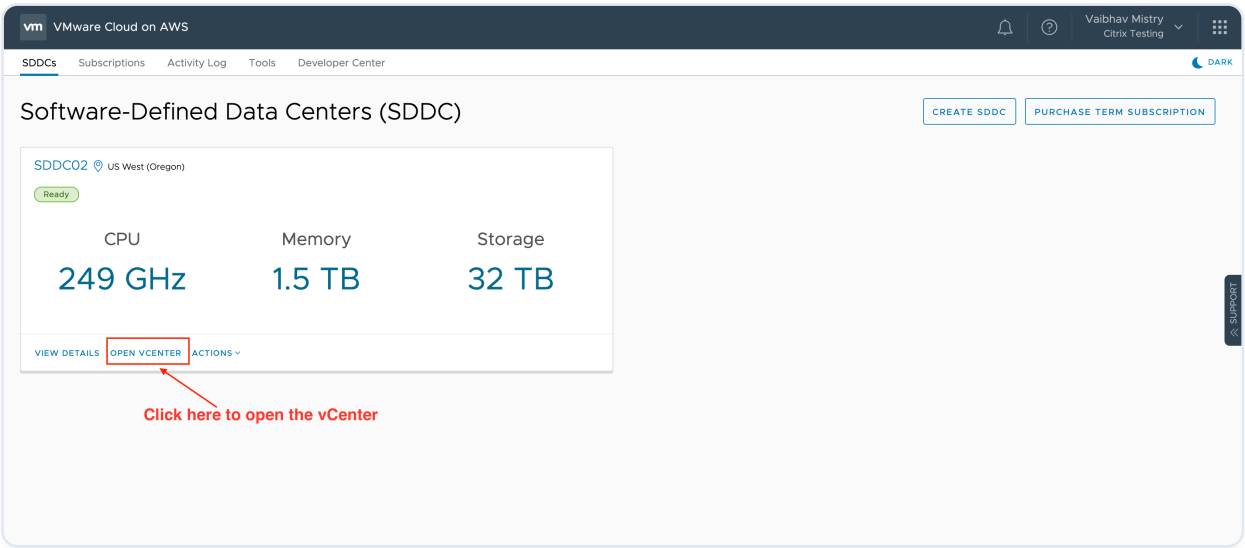
1. Faça login nos serviços de nuvem VMware usando o URL `<https://console.cloud.vmware.com/>`.

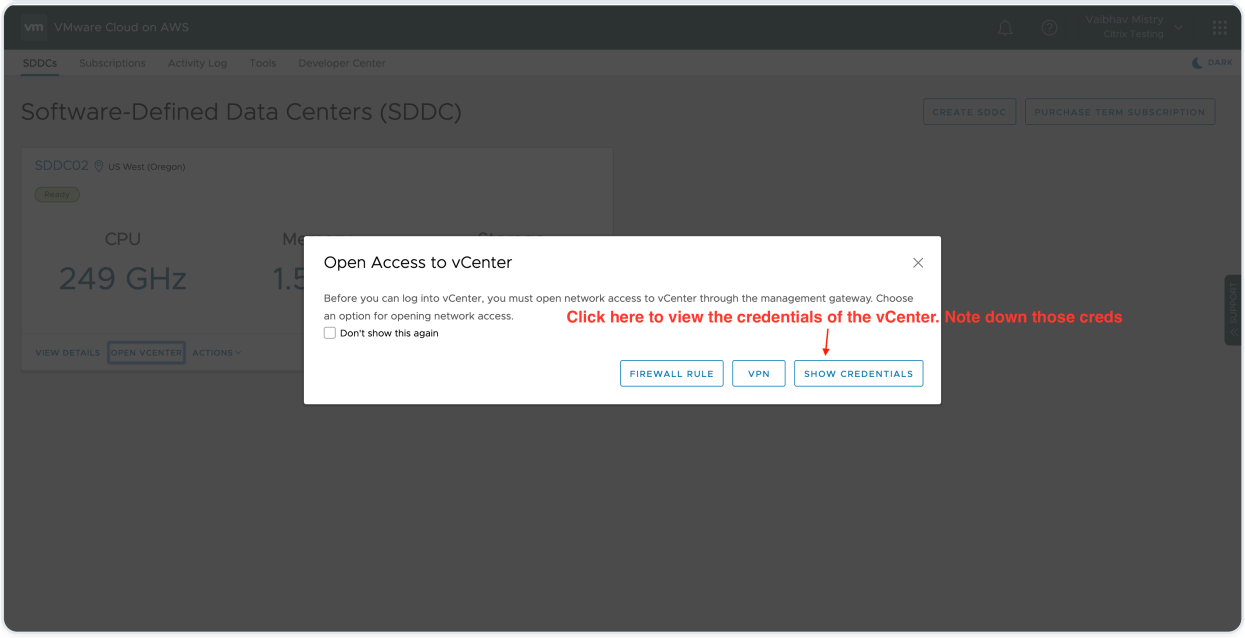



2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

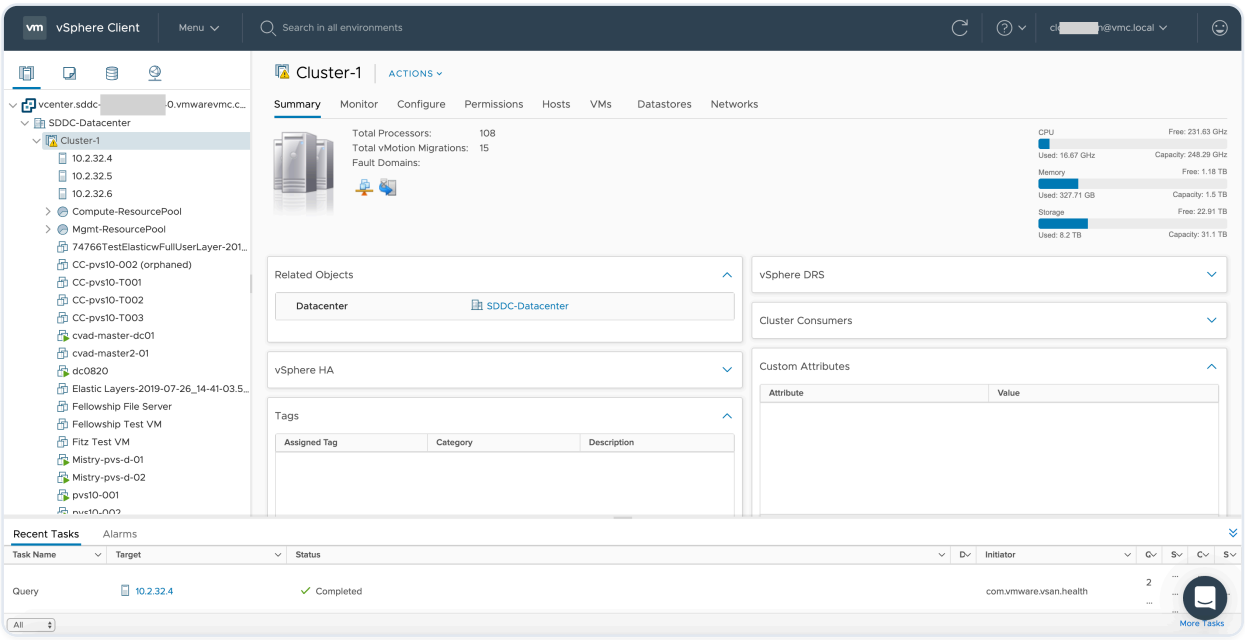



3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Anote as credenciais para uso posterior.



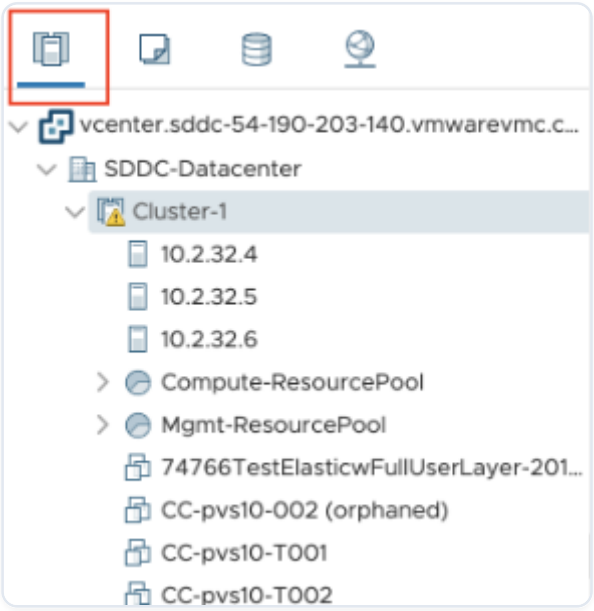

4. Abra um navegador da Web e insira o URL do vSphere Web Client.
5. Insira as credenciais conforme observado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



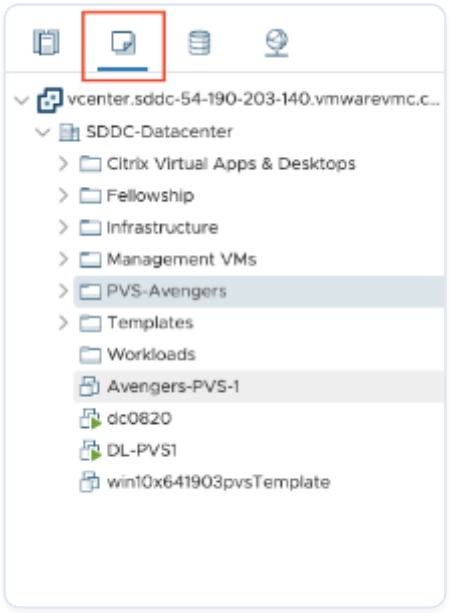

## Sobre o ambiente de nuvem VMware

Existem quatro visualizações na página da Web do cliente vSphere.

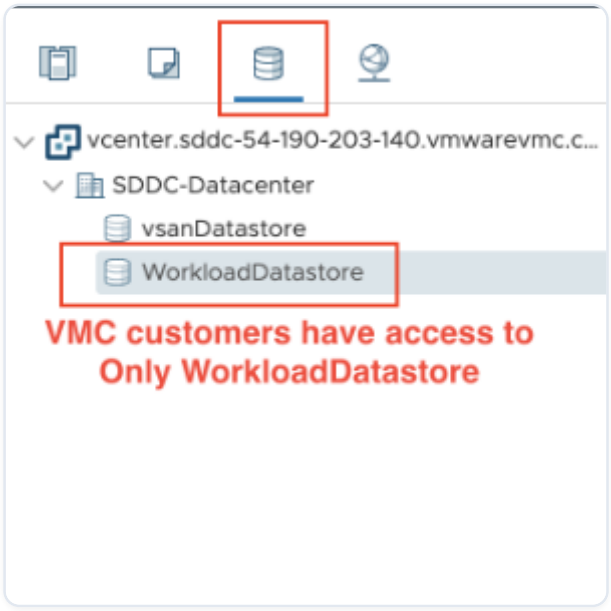
- Visualização de Host e Cluster: Você não pode criar um novo Cluster, mas o administrador da nuvem pode criar vários pools de recursos.



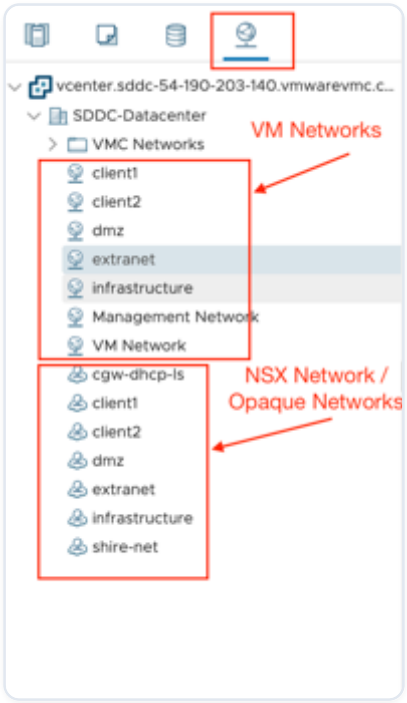

- Visualização de VM e Modelo: O administrador da nuvem pode criar muitas pastas.




- Visualização de Armazenamento: Selecione o armazenamento **WorkloadDatastore** ao adicionar a unidade de hospedagem no Citrix Studio porque você tem acesso apenas ao Workload Datastore.




- Visualização de Rede: Os ícones são diferentes para redes de nuvem VMware e redes opacas.




Depois de configurar o cluster, consulte Ambientes de virtualização VMware para adicionar conexões e recursos.

### Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão, consulte Conexão com soluções de nuvem e parceiros VMware

### Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

# Instalar componentes principais

> **Importante:**
>
> A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade de licença. Para obter mais informações, consulte Dados de Licenciamento da Citrix. Certifique-se de que o Servidor de Licenças esteja executando

> no mínimo a versão 11.17.2 build 53100. O não cumprimento deste pré-requisito pode causar erros ou recomendações durante as atualizações e criação do site.

> Os componentes principais são o Citrix Delivery Controller™, Citrix Studio, Web Studio, Citrix Director e Citrix License Server.

> **Observação:**

> O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio — um console de gerenciamento baseado na web que oferece paridade total de recursos com o Citrix Studio. Para obter mais informações sobre o Web Studio, consulte Instalar o Web Studio.

> (Em versões anteriores a 2003, os componentes principais incluíam o Citrix StoreFront. Você ainda pode instalar o StoreFront clicando no bloco **Citrix StoreFront** ou executando o comando disponível na mídia de instalação.)

Antes de iniciar uma instalação, revise este artigo e Prepare-se para instalar.

Este artigo descreve a sequência do assistente de instalação ao instalar os componentes principais. Equivalentes de linha de comando são fornecidos. Para obter mais informações, consulte Instalar usando a linha de comando.

## Etapa 1. Baixe o software do produto e inicie o assistente

Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.

Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.

Faça logon na máquina onde você está instalando os componentes principais, usando uma conta de administrador local.

Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não iniciar automaticamente, clique duas vezes no aplicativo **AutoSelect** ou na unidade montada.

## Etapa 2. Escolha qual produto instalar

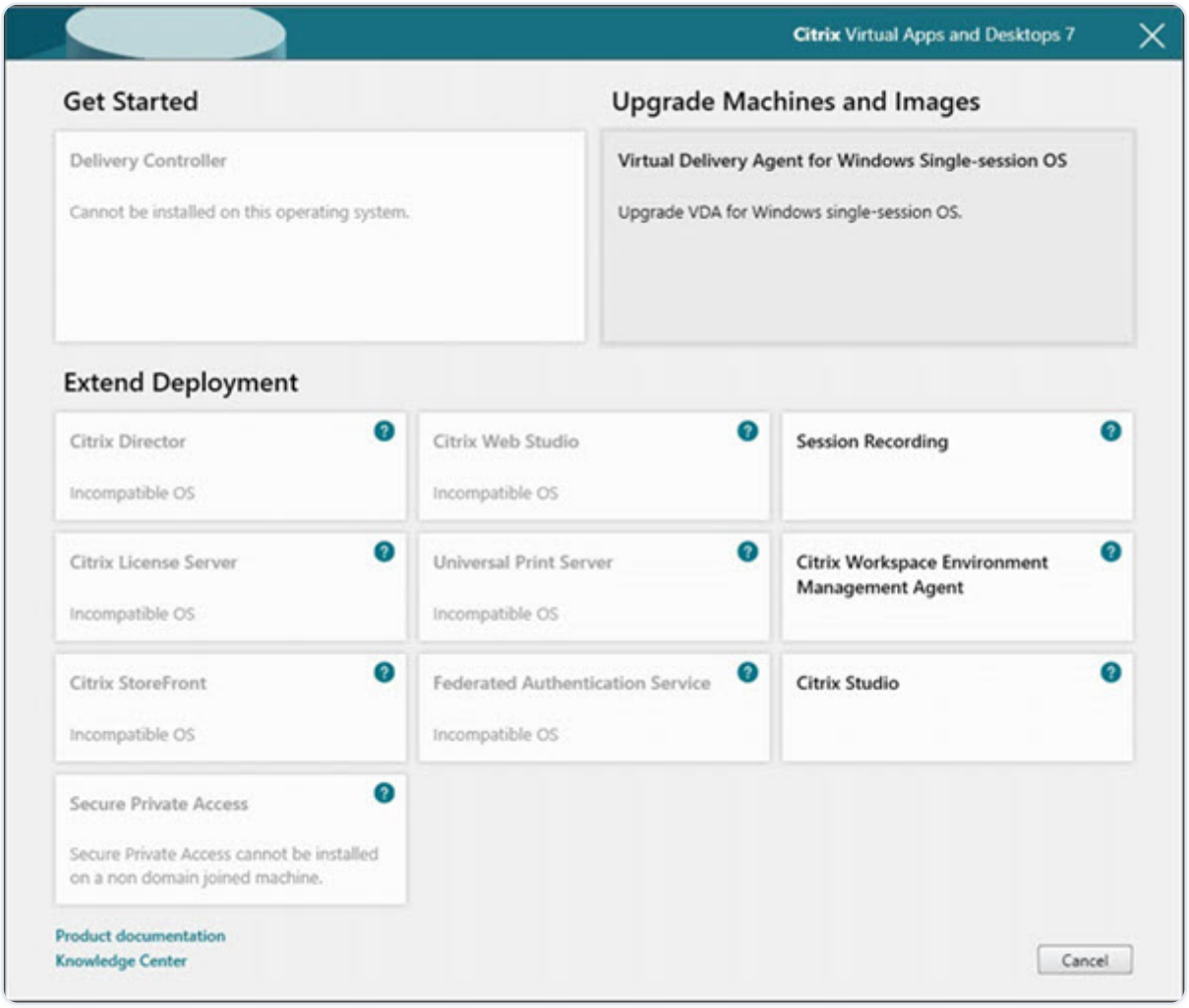



Clique em **Iniciar** ao lado do produto a ser instalado: Virtual Apps ou Virtual Apps and Desktops.

(Se a máquina já tiver componentes do Citrix Virtual Apps and Desktops instalados, esta página não aparecerá.)

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

## Etapa 3. Escolha o que instalar

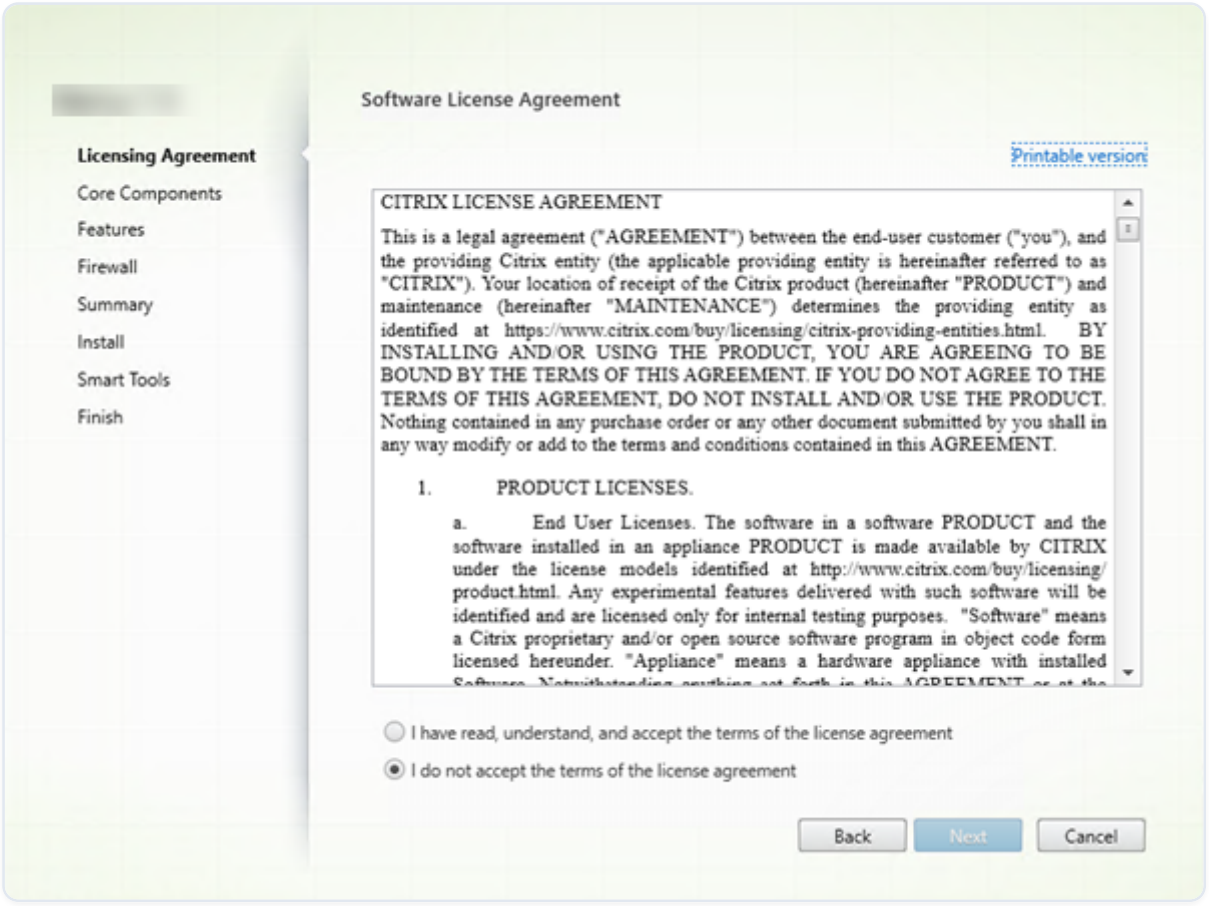



Se você está apenas começando, selecione **Delivery Controller**. (Em uma página posterior, você selecionará os componentes específicos a serem instalados nesta máquina.)

Se você já instalou um Controller (nesta máquina ou em outra) e deseja instalar outro componente, selecione o componente na seção **Estender Implantação**.

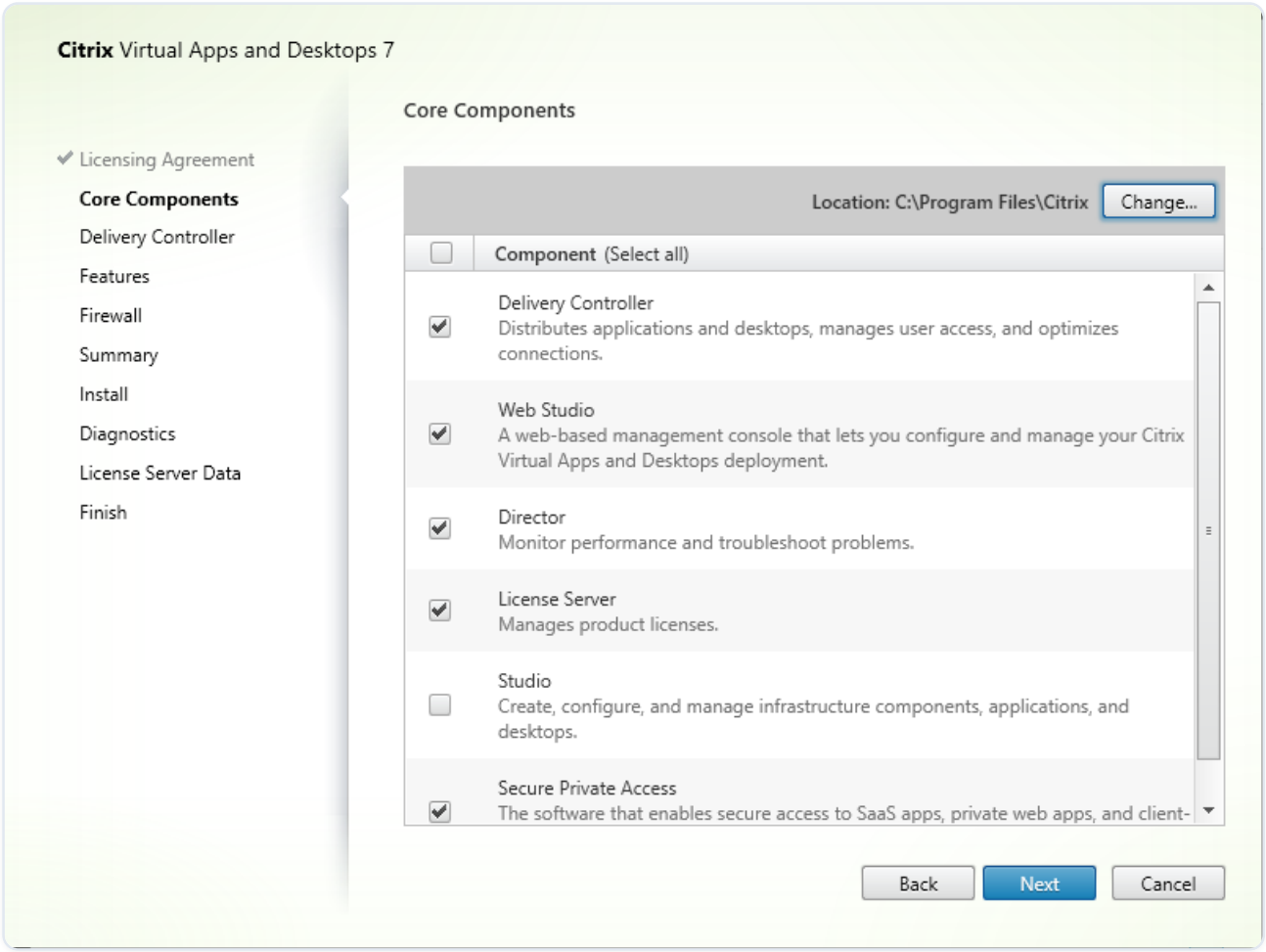
Opção de linha de comando: `/components`

## Etapa 4. Leia e aceite o contrato de licença




Na página **Contrato de Licença**, depois de ler o contrato de licença, indique que você o leu e aceitou. Em seguida, clique em **Avançar**.

## Etapa 5. Selecione os componentes a serem instalados e o local de instalação




Na página **Componentes principais**:

- **Local:** Por padrão, os componentes são instalados em `C:\Program Files\Citrix`. O padrão é adequado para a maioria das implantações. Se você especificar um local diferente, ele deve ter permissões de execução para o serviço de rede.
- **Componentes:** Por padrão, as caixas de seleção para todos os componentes principais são selecionadas. A instalação de todos os componentes principais em um servidor é adequada para prova de conceito, teste ou pequenas implantações de produção. Para ambientes de produção maiores, a Citrix recomenda instalar o Director, StoreFront, Secure Private Access e o License Server em servidores separados.

> **Observação:**
>
> Se você estiver instalando componentes em mais de um servidor, instale o Citrix License Server e as licenças primeiro, antes de instalar outros componentes em outros servidores. Para obter orientação, consulte a seção Instalação automática do Guia de Licenciamento para Citrix Virtual Apps and Desktops.

> Um ícone o alerta quando você opta por não instalar um componente principal necessário nesta máquina. Esse alerta o lembra de instalar esse componente, embora não necessariamente nesta máquina.

Clique em **Avançar**.

Opções de linha de comando: `/installdir`, `/components`, `/exclude`

### Verificação de hardware

Ao instalar ou atualizar um Delivery Controller, o hardware é verificado. O instalador o alerta se a máquina tiver menos RAM do que o recomendado (5 GB), o que pode afetar a estabilidade do site. Para obter mais informações, consulte Requisitos de hardware.

**Interface gráfica:** Uma caixa de diálogo é exibida.

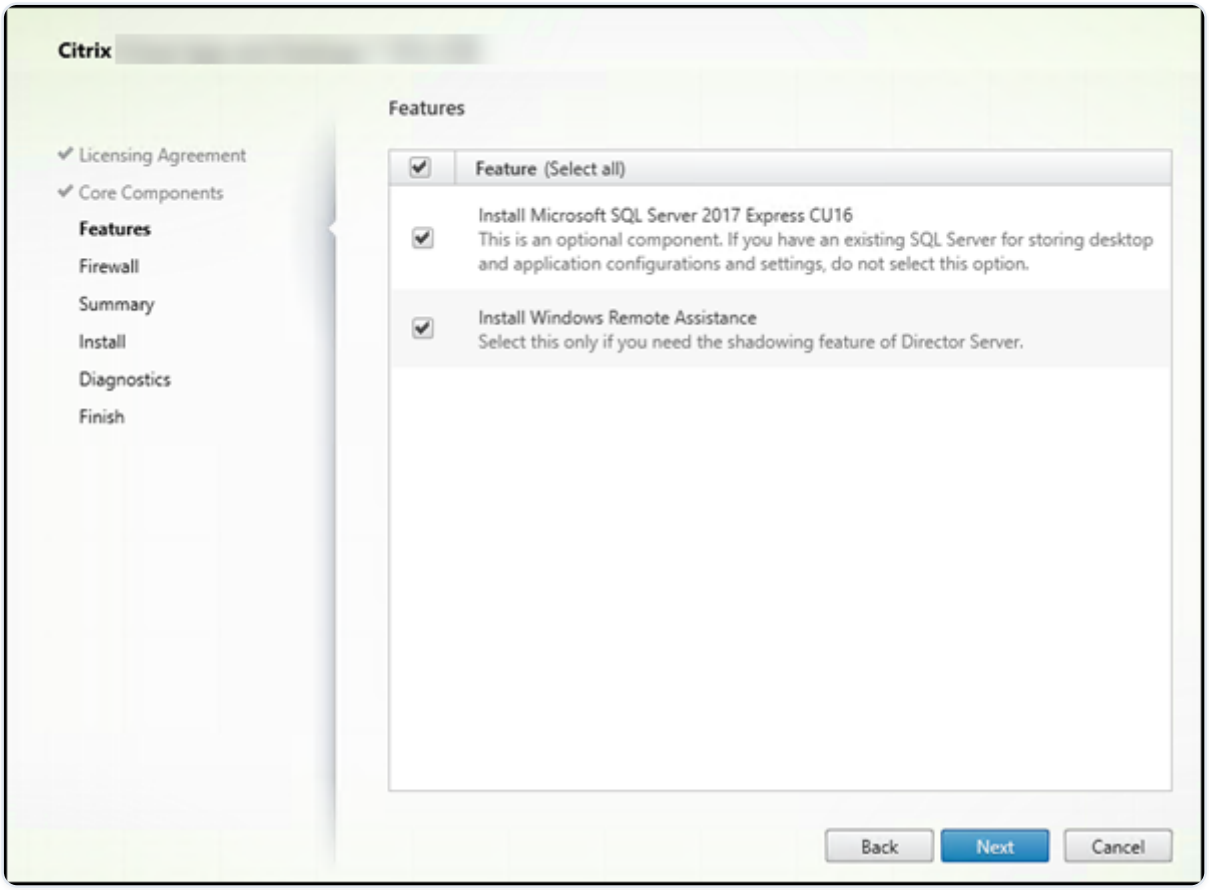
- Recomendado: Clique em **Cancelar** para interromper a instalação. Adicione mais RAM à máquina e inicie a instalação novamente.
- Alternativamente, clique em **Avançar** para continuar com a instalação. O site pode apresentar problemas de estabilidade.

**Interface de linha de comando:** A instalação/atualização termina. Os logs de instalação contêm uma mensagem que descreve o que foi encontrado e as opções disponíveis.

- Recomendado: Adicione mais RAM à máquina e execute o comando novamente.
- Alternativamente, execute o comando novamente com a opção `/ignore_hw_check_failure` para ignorar o aviso. Seu site pode apresentar problemas de estabilidade.

Ao atualizar, você também é notificado se a versão do SO ou do SQL Server não é mais suportada. Consulte Atualizar uma implantação.

## Etapa 6. Habilitar ou desabilitar recursos



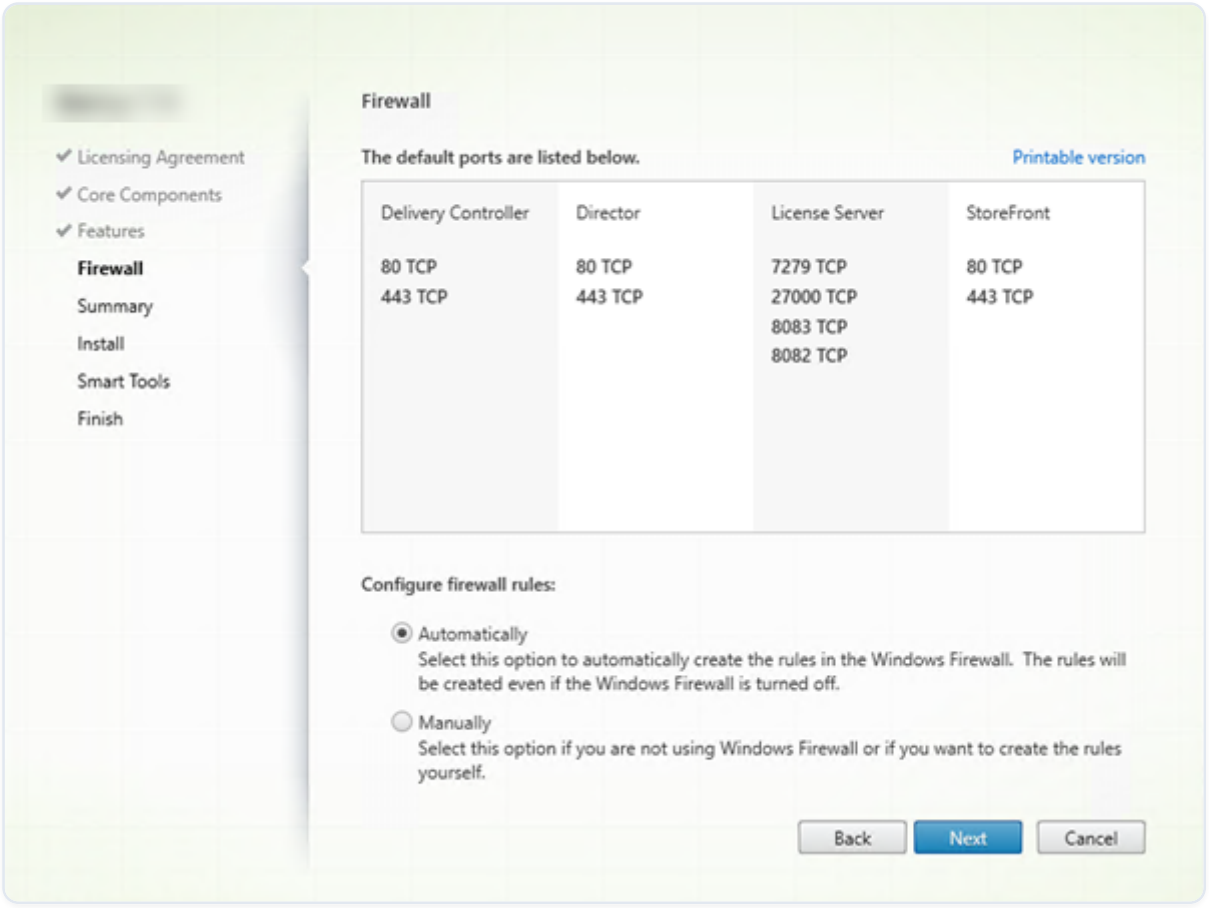

Na página **Recursos**:

- Escolha se deseja instalar o Microsoft SQL Server Express para usar como banco de dados do site. Por padrão, esta seleção está ativada. Se você não estiver familiarizado com os bancos de dados do Citrix Virtual Apps and Desktops, consulte Bancos de dados.
- Ao instalar o Director, o Assistência Remota do Windows é instalado automaticamente. Você escolhe se deseja habilitar o shadowing no Assistência Remota do Windows para uso com o shadowing de usuário do Director. Habilitar o shadowing abre a porta TCP 3389. Por padrão, este recurso está habilitado. A configuração padrão é adequada para a maioria das implantações. Este recurso aparece somente quando você está instalando o Director.

Clique em **Avançar**.

Opções de linha de comando: `/nosql` (para evitar a instalação), `/no_remote_assistance` (para evitar a habilitação)

## Etapa 7. Abrir portas do firewall do Windows



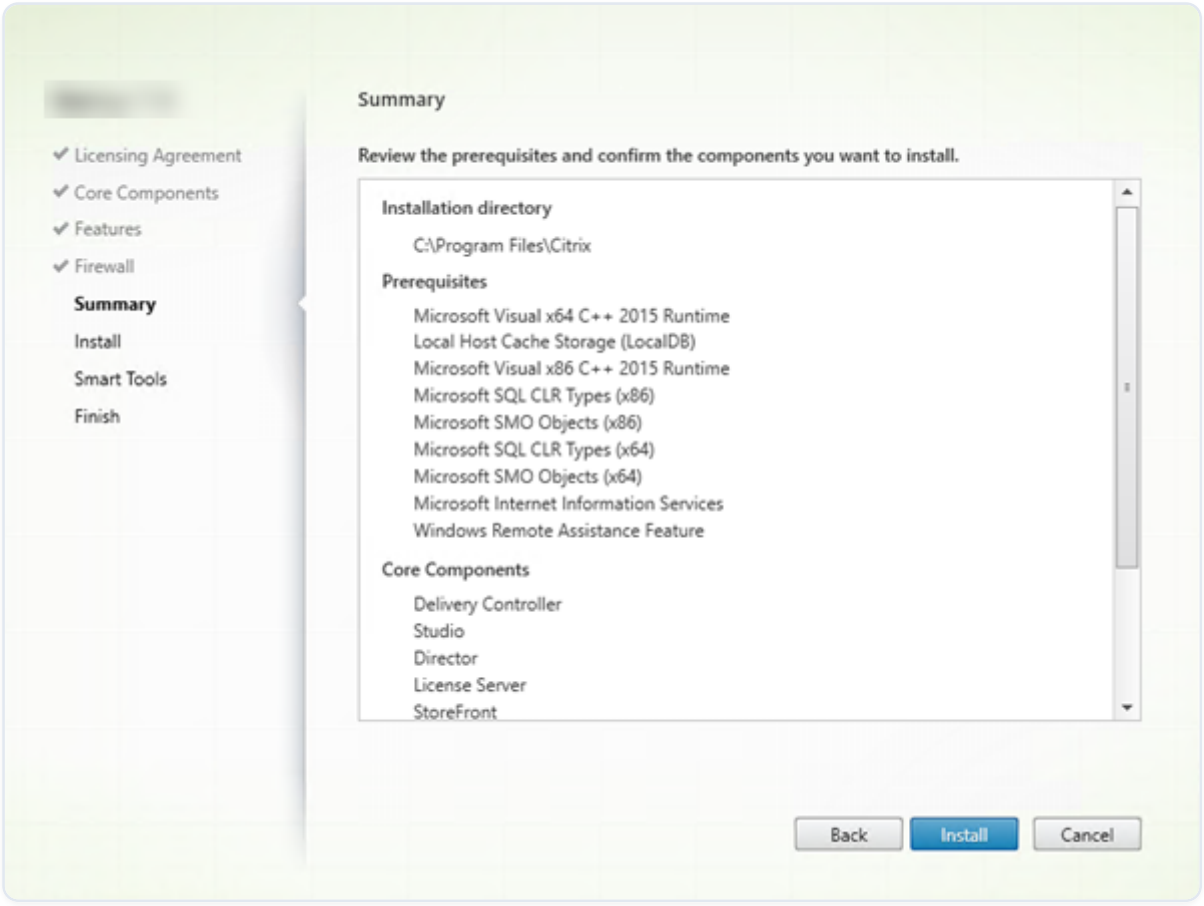

Por padrão, as portas na página **Firewall** são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja habilitado. A configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

(O gráfico mostra as listas de portas quando você instala todos os componentes principais nesta máquina. Esse tipo de instalação geralmente é apenas para implantações de teste.)

Opção de linha de comando: `/configure_firewall`

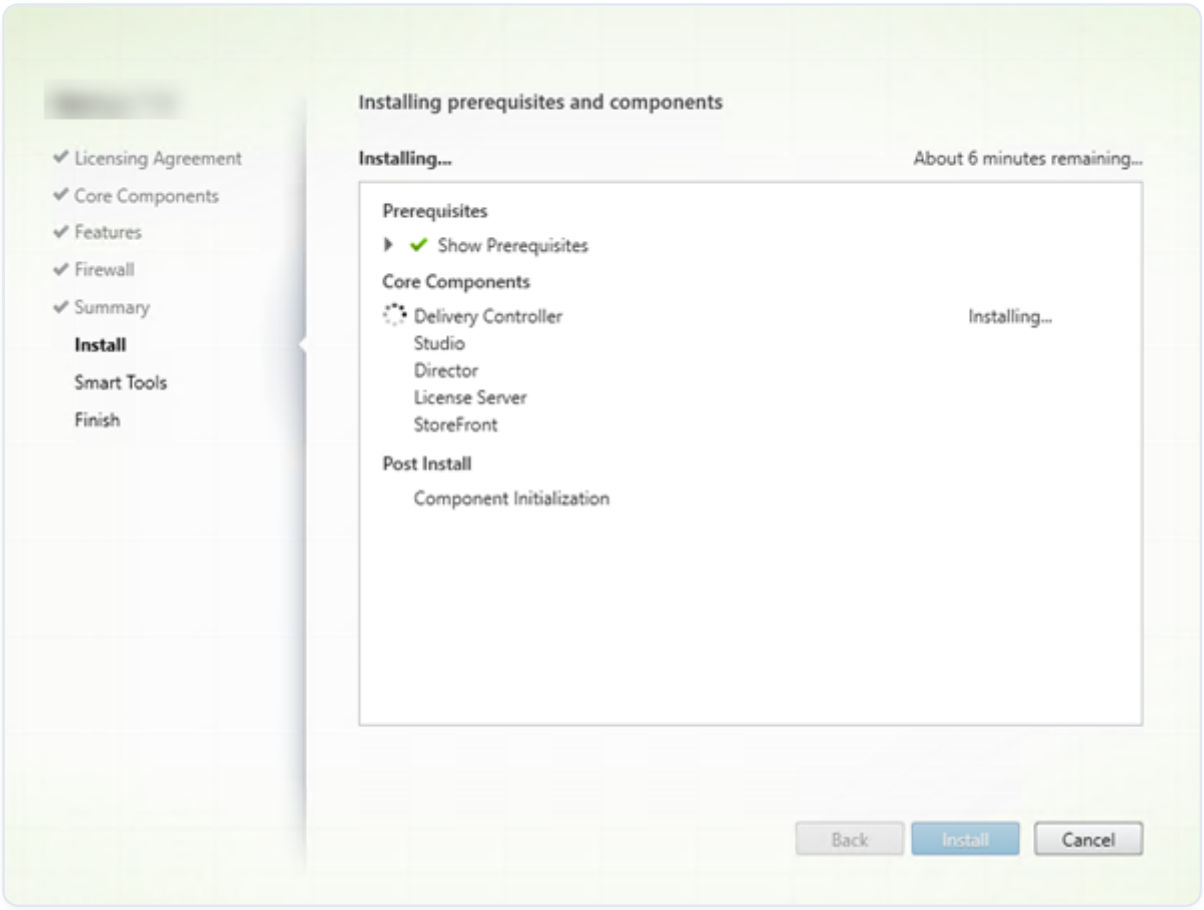
## Etapa 8. Revisar pré-requisitos e confirmar a instalação



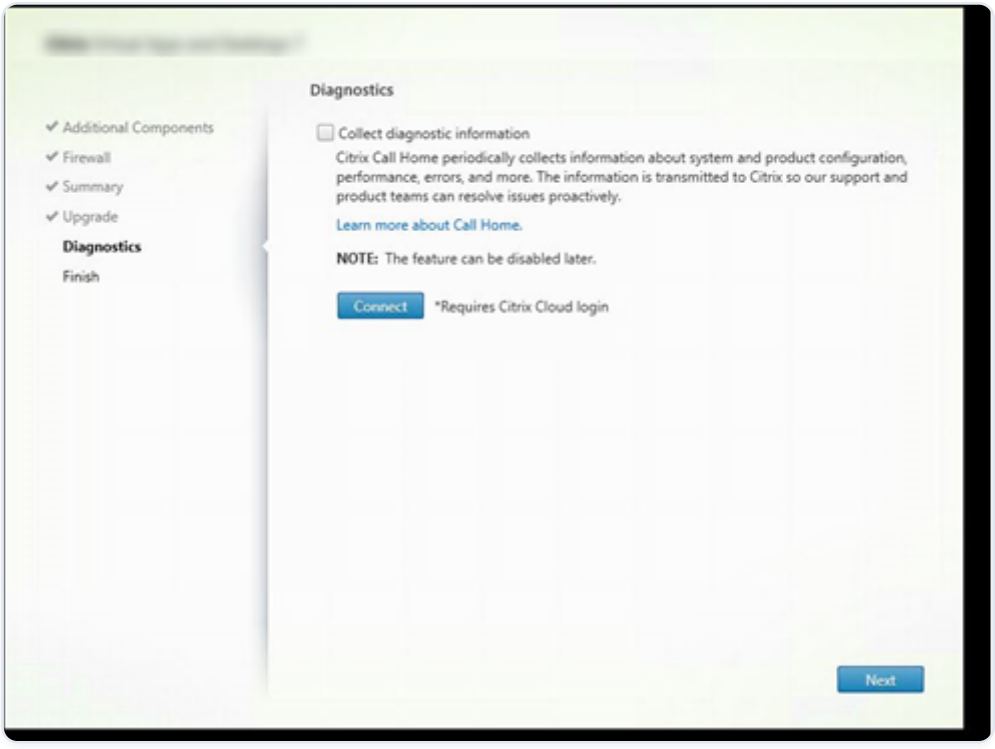

A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções, se necessário.

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

A exibição mostra o progresso da instalação:




## Etapa 9. Compartilhando informações de diagnóstico com o Cloud Software Group




Na página **Diagnóstico**, escolha se deseja participar do Citrix Call Home.

Esta página aparece ao instalar um Delivery Controller usando a interface gráfica. Ao instalar o StoreFront (mas não um Controller), o assistente exibe esta página. Ao instalar outros componentes principais (mas não um Controller ou StoreFront), o assistente não exibe esta página.

Durante uma atualização, esta página não aparece se o Call Home já estiver ativado ou se o instalador encontrar um erro relacionado ao Citrix Telemetry Service.

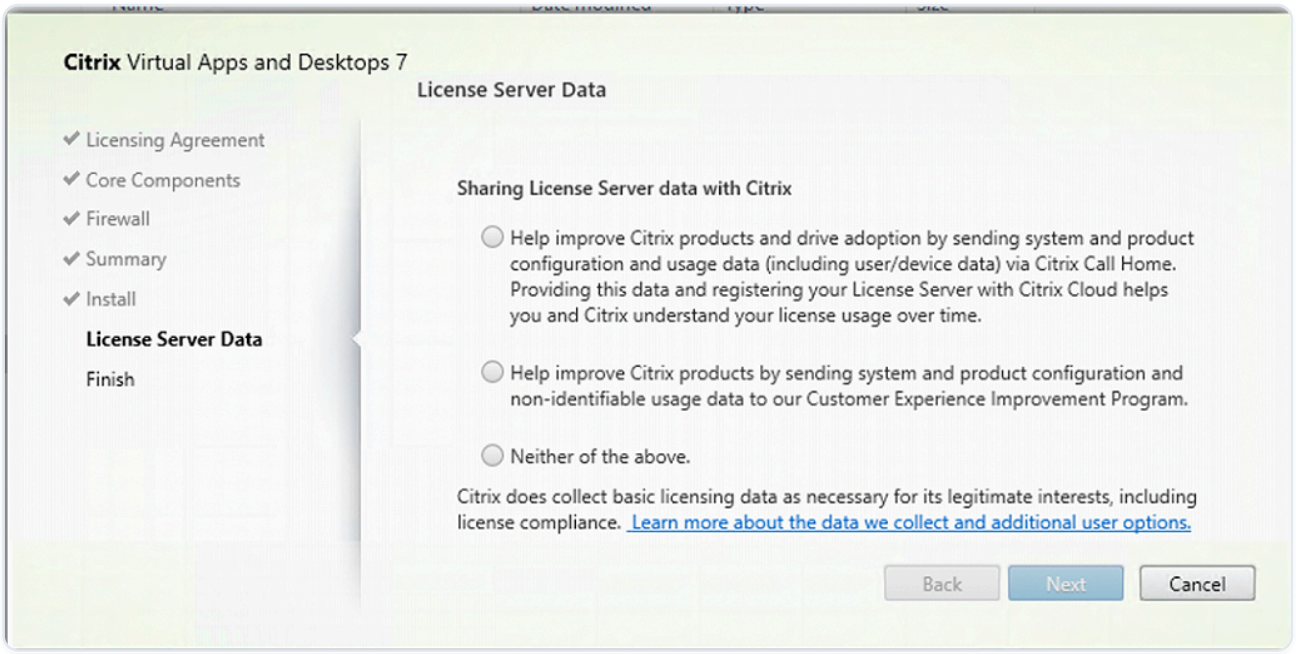
Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix. Você pode alterar sua escolha de inscrição posteriormente, após a instalação.

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

Se você clicar em **Conectar** na página **Diagnóstico** sem primeiro selecionar **Coletar informações de diagnóstico**, depois de fechar a caixa de diálogo **Conectar aos Serviços Citrix Insight**, o botão **Avançar** será desativado. Você não pode ir para a próxima página. Para reativar o botão **Avançar**, selecione e desmarque imediatamente **Coletar informações de diagnóstico**.

Para obter mais informações, consulte Call Home.

## Etapa 10. Compartilhamento de dados do License Server com o Cloud Software Group




Na página **Dados do License Server**, solicitamos que você compartilhe dados do Call Home ou dados do Programa de Melhoria da Experiência do Cliente (CEIP) para nos ajudar. Além disso, o

Cloud Software Group também exige a coleta de dados básicos de licenciamento, incluindo conformidade de licença, conforme necessário para seus interesses legítimos.

A página **Dados do License Server** aparece quando você instalou o License Server:

- Como autônomo.
- Como um componente principal, durante a instalação de um Delivery Controller.

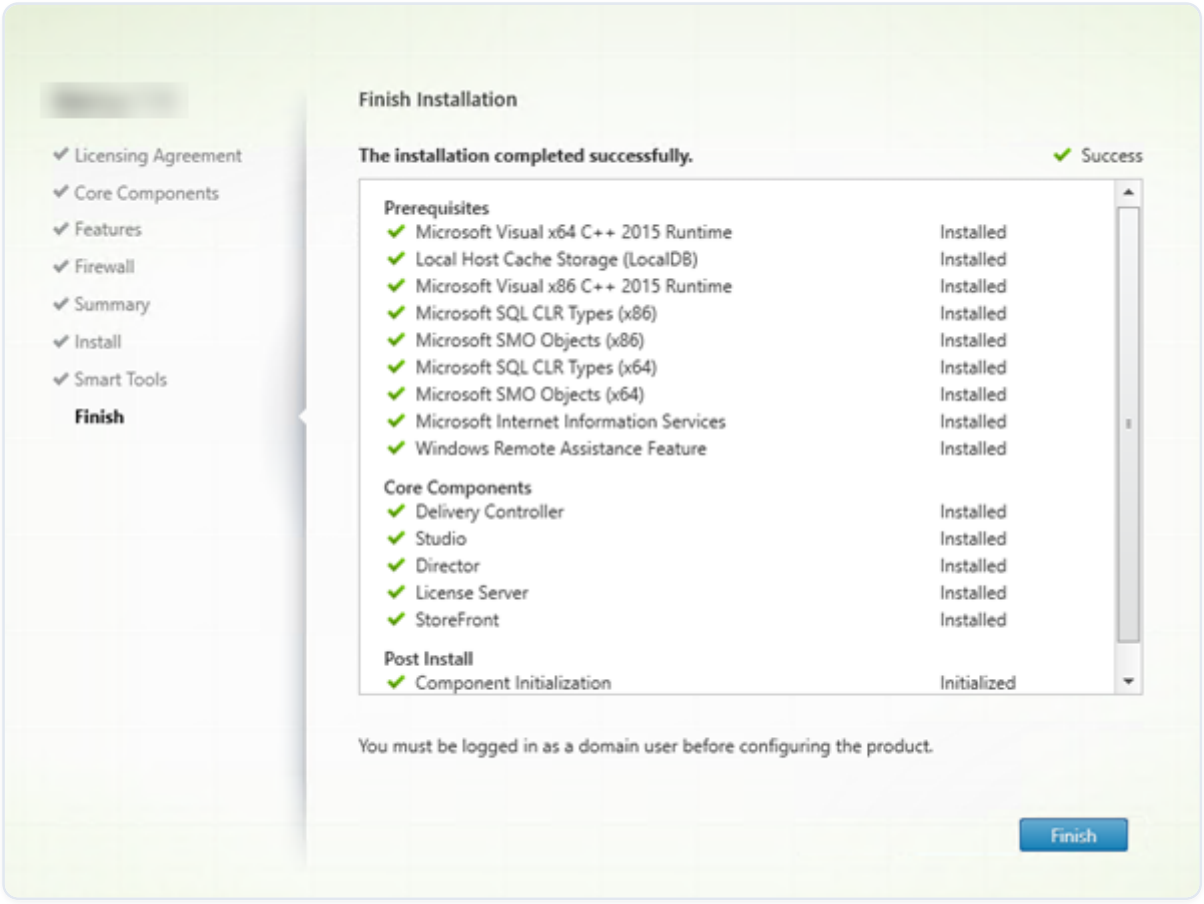
Durante uma atualização, esta página não aparece se a configuração já estiver definida no arquivo `/CITRIX.opt:`.

O License Server monitora vários tipos de dados do usuário, como dados de licenciamento, dados do Call Home e dados do CEIP. Para habilitar a coleta de dados do Call Home e do CEIP, você deve optar por participar (opt-in).

Para obter mais informações sobre como habilitar a coleta de dados do Call Home e do CEIP ao instalar usando a linha de comando, consulte Opções de linha de comando para instalar componentes principais.

Para obter mais informações sobre a coleta de dados de licenciamento do Cloud Software Group, consulte Programas de coleta de dados de licenciamento do Citrix.

## Etapa 11. Concluir esta instalação




A página **Concluir** contém marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com sucesso.

Clique em **Concluir**.

## Etapa 12. Instalar os componentes principais restantes em outras máquinas

Se você instalou todos os componentes principais em uma máquina, continue com Próximas etapas. Caso contrário, execute o instalador em outras máquinas para instalar outros componentes. Você também pode instalar mais Controladores em outros servidores.

## Próximas etapas

Depois de instalar todos os componentes necessários, use o Studio para criar um site.

Após criar o site, instale os VDAs.

A qualquer momento, você pode usar o instalador completo do produto para estender sua implantação com os seguintes componentes:

- **Componente de servidor Universal Print Server:** Inicie o instalador no seu servidor de impressão.

a. Selecione **Universal Print Server** na seção **Estender Implantação**.

b. Aceite o contrato de licença.

c. Na página **Firewall**, por padrão, as portas TCP 7229 e 8080 são abertas no firewall se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Você pode desativar essa ação padrão se quiser abrir as portas manualmente.

Para instalar este componente a partir da linha de comando, consulte Opções de linha de comando para instalar um Universal Print Server.

- Serviço de Autenticação Federada.
- Gravação de Sessão.
- Gerenciamento de Ambiente de Workspace.

# Instalar o Web Studio

## Introdução

O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio — um console de gerenciamento baseado na web que oferece paridade total de recursos com o Citrix Studio. Com a mesma aparência e funcionalidade da interface do Citrix DaaS Studio, o Web Studio moderniza sua experiência de gerenciamento, fornecendo uma experiência web nativa.

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

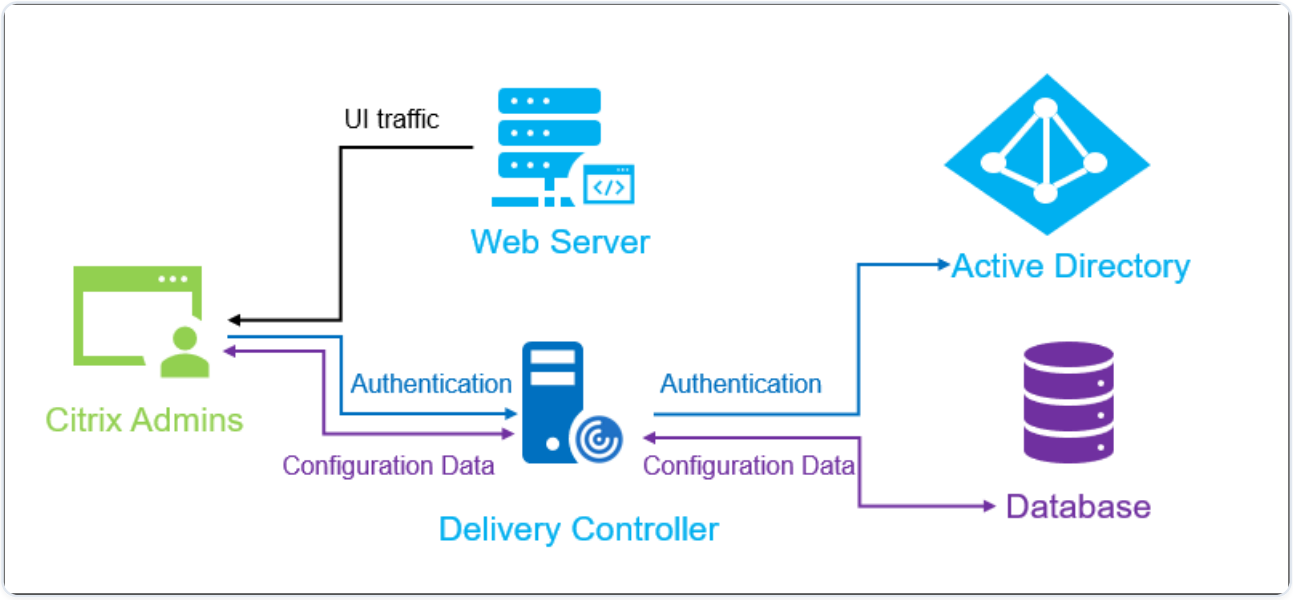
- Instalado em um servidor dedicado:

  Para ambientes maiores onde o desempenho e a escalabilidade são críticos, recomendamos instalar o Web Studio em um servidor dedicado. Este servidor também pode, opcionalmente, hospedar o Director.

- Integrado com um Delivery Controller™:

  Para implantações rápidas e ambientes mais simples, instale o Web Studio diretamente em um Delivery Controller. Essa abordagem é ideal para implantações menores, onde minimizar a sobrecarga administrativa é uma prioridade.

O diagrama a seguir mostra a arquitetura do Web Studio:




Um fluxo de trabalho geral para colocar o Web Studio em funcionamento é o seguinte:

1. Instalar o Web Studio.
2. Configurar um certificado para TLS.
3. Configurar um site.
4. Adicionar Delivery Controllers ao Web Studio para gerenciamento.
5. (Opcional) Configurar o Web Studio como um proxy para Delivery Controllers
6. (Opcional) Desativar Pendo(#optional-enable-or-disable-pendo).
7. Fazer login no Web Studio(#sign-in-to-web-studio).

Para configurar uma implantação do Web Studio com balanceamento de carga, consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-core/load-balance-studio.html).

### Novos recursos disponíveis no Web Studio

Consulte o artigo (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/whats-new.html#web-studio).

### Requisitos do sistema

Sistemas operacionais suportados:

- Windows Server 2022, Edições Standard e Datacenter, e com a opção Server Core
- 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
- Safari 14

A resolução de tela ideal recomendada para visualizar o Web Studio é 1440 x 1024.

### Pré-requisitos

Esta versão do Web Studio é compatível com implantações do Citrix Virtual Apps and Desktops™ 2212 e posteriores.

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

### Limitações conhecidas

Se você usa o Web Studio e o Citrix Studio de forma intercambiável, considere a seguinte limitação: Um modelo criado no Web Studio não é exibido no Citrix Studio, e vice-versa. Isso ocorre porque o Web Studio usa um banco de dados diferente do Citrix Studio para armazenar modelos. Como solução alternativa, crie uma política a partir de um modelo no Web Studio e, em seguida, crie um modelo a partir dessa política no Citrix Studio, e vice-versa.

- Para garantir uma instalação bem-sucedida do Web Studio, não altere o nome do site padrão (**Default Web Site**) no Gerenciador de Serviços de Informações da Internet (IIS). Quaisquer alterações no nome do site padrão resultam em falhas de instalação.

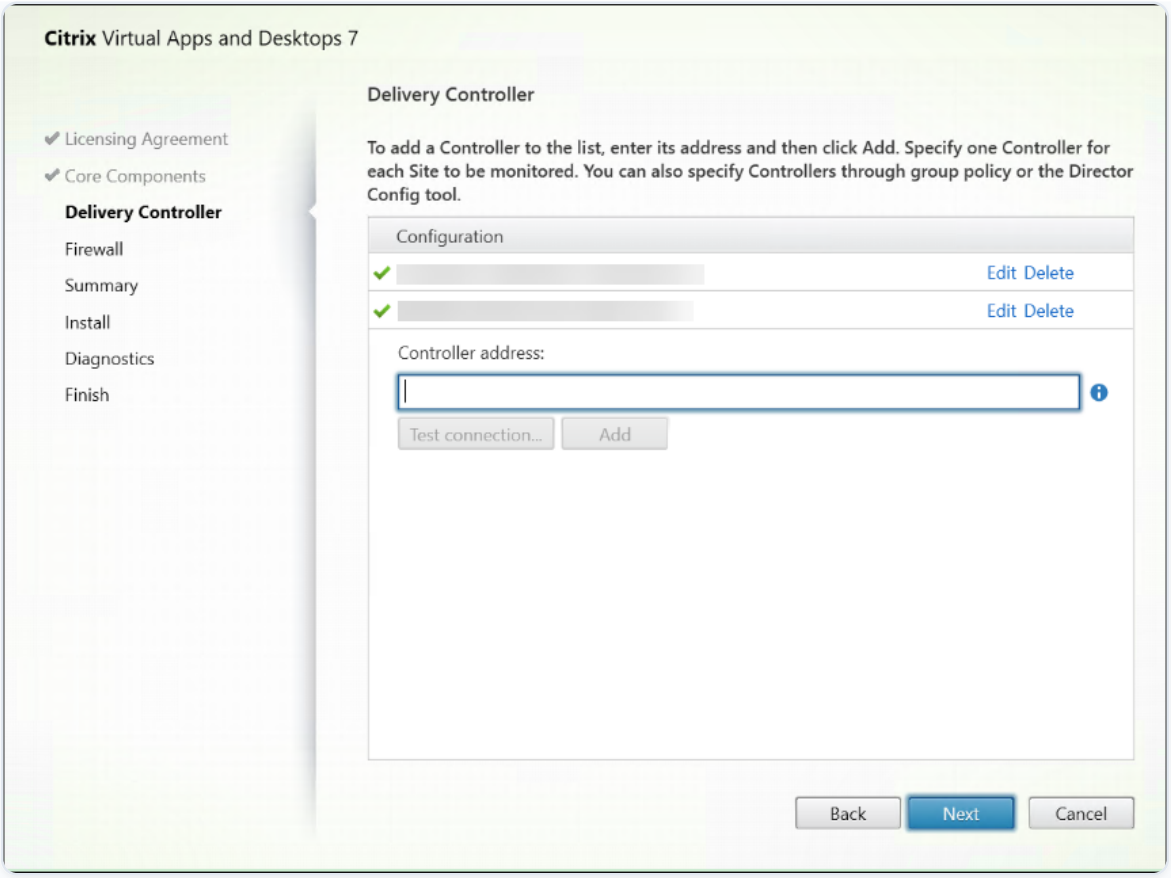
### Instalar o Web Studio

As informações a seguir são um suplemento às orientações em Instalar componentes principais. Para instalar o Web Studio:

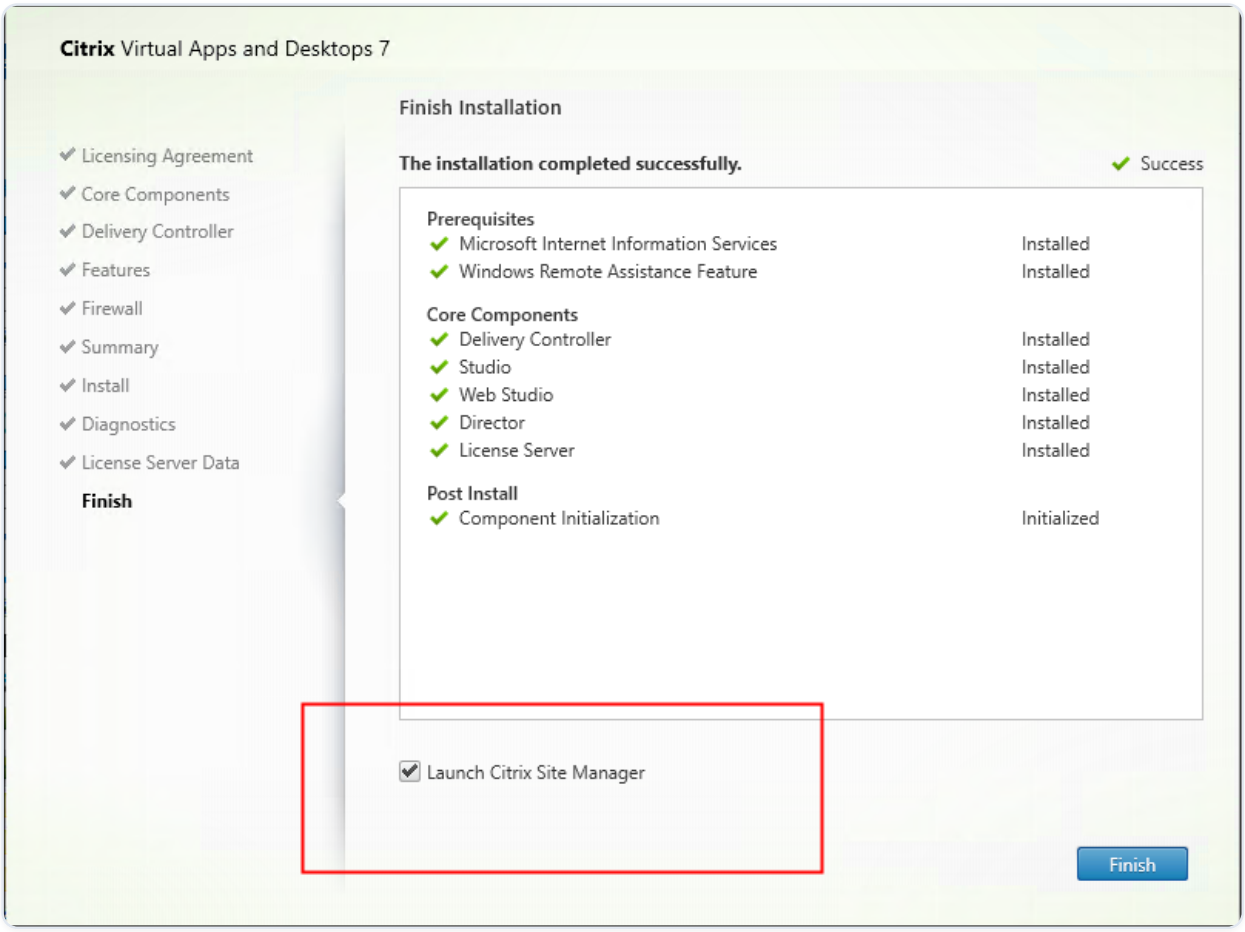
- Instale o Web Studio usando o instalador ISO completo do produto para Citrix Virtual Apps and Desktops. O instalador ISO verifica os pré-requisitos, instala quaisquer componentes ausentes, configura o site do Web Studio (no Delivery Controller, se incluído na instalação do Delivery Controller) e executa a configuração básica.
- Se o Web Studio não foi incluído durante a instalação, use o instalador para adicionar o Web Studio.
- Ao instalar o Web Studio, você será solicitado a digitar o FQDN de um Delivery Controller.

> **Observação:**

- Você pode adicionar mais de um Delivery Controller. O Web Studio tenta se conectar a eles em ordem aleatória. Se o Delivery Controller ao qual o Web Studio está tentando se conectar estiver inacessível, o Web Studio automaticamente recorrerá a outros Delivery Controllers.
- Se o Director foi selecionado em **Core Components** e instalado, os Delivery Controllers que você adicionar aqui serão usados tanto para o Web Studio quanto para o Director.
- Se o delivery controller estiver configurado para TLS (recomendado), o FQDN inserido deve corresponder ao nome comum ou a um nome alternativo de assunto do certificado instalado no delivery controller.




- Na página **Concluir**, a caixa de seleção **Iniciar Gerenciador de Sites** é selecionada por padrão para que o Citrix Site Manager seja aberto automaticamente. Para iniciá-lo mais tarde, abra o menu Iniciar da sua área de trabalho e selecione **Citrix > Citrix Site Manager**. Antes de iniciar o Web Studio, você precisa usar o Citrix Site Manager para criar um site ou ingressar em um site existente. Para obter mais informações, consulte Configurar um site.




**Observação:**

Você também pode usar a linha de comando para instalar o Web Studio. Exemplo: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`. Para obter mais informações, consulte Instalar usando a linha de comando.

### Configurar um certificado para TLS

Por padrão, se o IIS ainda não estiver configurado para HTTPS, o instalador cria um certificado autoassinado usando o FQDN do servidor como nome comum do certificado e o vincula à porta 443. Esse comportamento permite que os usuários acessem o Web Studio da máquina local, mas os usuários que se conectam de outras máquinas veem avisos de segurança porque o certificado não é confiável. Recomendamos substituir este certificado por um certificado assinado por uma autoridade de certificação (CA) empresarial ou pública. Para obter mais informações, consulte Habilitar TLS no Web Studio e no Director. Se um certificado TLS já estiver configurado no IIS, o instalador não fará alterações.

### Configurar um site

Para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como um site), use a ferramenta Citrix Site Manager. A ferramenta é instalada automaticamente com um Delivery Controller.

Para configurar um site, siga estas etapas:

1. Em um Delivery Controller, abra o menu Iniciar da área de trabalho e selecione **Citrix > Citrix Site Manager**.
2. No Citrix Site Manager, selecione **Create a site**. O assistente de configuração do site é exibido.
3. Crie um site e configure suas definições da seguinte forma:
   - Na página **Introduction**, digite um nome para o site.
   - A página **Databases** contém seleções para configurar o site, o monitoramento e os bancos de dados de registro de configuração. Para obter mais informações, consulte Etapa 3. Bancos de dados.
   - Na página **Licensing**, especifique o endereço do License Server 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 Controller é adicionado automaticamente ao site.

> **Observação:**
>
> O usuário que cria um site se torna um administrador completo para ele. Para obter mais informações, consulte Administração delegada.

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

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

### Adicionar Delivery Controllers ao Web Studio para gerenciamento

Use a ferramenta de configuração do Studio para adicionar os Delivery Controllers ao Web Studio para gerenciamento. Esta ferramenta está disponível na pasta de instalação do Web Studio.

Por padrão, a ferramenta é instalada na seguinte pasta padrão.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Suponha que você queira configurar os dois Delivery Controllers a seguir para o site que você deseja gerenciar com o Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Execute o seguinte comando PowerShell:

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

**Observação:**

- A ferramenta requer permissões de administrador do computador.
- As alterações de configuração do Delivery Controller podem não ter efeito imediato devido às configurações de cache no servidor IIS. Para efeito imediato, vá para o servidor Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegar para *Server_name* **> Sites > Default Web Site**, e selecione **Reiniciar** no painel Gerenciar Site.
- Ao reimplantar os Delivery Controllers com novos FQDNs, atualize seus FQDNs no Web Studio usando `StudioConfig.exe` e no arquivo `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json`. Se você não atualizar o arquivo `manifest.json`, os FQDNs antigos ainda aparecerão na janela de login do Web Studio. Como resultado, você deve inserir os novos FQDNs como uma alternativa ao fazer login.
- Para visualizar todos os parâmetros suportados, execute `StudioConfig.exe --help`.

### (Opcional) Configurar o Web Studio como um proxy para Delivery Controllers

Por padrão, ao gerenciar sua implantação usando o console do Web Studio, você se conecta ao servidor Web Studio e aos Delivery Controllers por meio do navegador da web. Oferecemos uma opção para configurar o servidor Web Studio como um proxy para Delivery Controllers. Como resultado, você se conecta apenas ao servidor Web Studio ao gerenciar sua implantação.

Esta seção o orienta a configurar um servidor Web Studio como um proxy para os Delivery Controllers. Assumimos que o Web Studio e os Delivery Controllers estão instalados em servidores diferentes.

Antes de começar, verifique se você tem todos os componentes principais necessários instalados em sua implantação. Para obter mais informações, consulte Instalar componentes principais.

Para habilitar o modo proxy para o Web Studio, siga estas etapas:

1. No servidor do Web Studio, execute o Windows PowerShell como administrador.
2. Execute o seguinte comando, substituindo `fqdn_of_webstudio_machine` pelo FQDN do seu servidor Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

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

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

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

### (Opcional) Habilitar ou desabilitar o Pendo

A partir da versão 2411, o Web Studio integra o Pendo, que é habilitado por padrão. O Pendo coleta seus dados de uso de acordo com a Política de Privacidade da Citrix. Ele também adiciona um ícone no canto inferior direito do Web Studio, fornecendo informações contextuais sobre recursos e opções de feedback. Se você preferir não compartilhar seus dados de uso, poderá desabilitar o Pendo usando a ferramenta de configuração do Studio.

Esta ferramenta está disponível na pasta de instalação do Web Studio. Por padrão, a ferramenta é instalada na seguinte pasta: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`.

Para desabilitar o Pendo, siga estas etapas:

1. Faça login no Web Studio. Se um ícone aparecer no canto inferior direito, o Pendo estará habilitado.
2. No servidor do Web Studio, execute o Windows PowerShell como administrador. Execute este comando do PowerShell:

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

Para habilitar o Pendo, execute este comando:

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

### Fazer login no Web Studio

1. Acesse o Web Studio em `https://<address of the server hosting Web Studio>/Citrix/Studio` se a porta padrão 443 for usada. Se uma porta diferente for configurada, use `https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio`.

   A página de login aparece se você adicionou Delivery Controllers ao Web Studio e eles estiverem acessíveis.

   > **Observação:**
   >
   > A página **Não é possível fazer login** aparece nos seguintes casos:
   >
   > - Nenhum Delivery Controller foi especificado para o site. Você será solicitado a adicionar um para se conectar.
   > - Os Delivery Controllers especificados estão inacessíveis. Clique em **Testar** para verificar a conectividade. Ou, insira um Delivery Controller alternativo e clique em **Conectar**.

2. Insira **Nome de usuário**, **Senha** e **Domínio**.
3. Clique em **Fazer login**.

### Próximas etapas

1. Instalar VDAs
2. Use o Web Studio para entregar aplicativos e desktops virtuais aos seus usuários por meio de:
    a. Criação de um catálogo de máquinas
    b. Criação de um grupo de entrega
    c. Criação de um grupo de aplicativos (opcional)

## Instalar usando a linha de comando

**Importante:**

- Se você estiver atualizando e sua versão atual usar ou tiver o software Personal vDisk ou AppDisks instalado, consulte Removendo PvD, AppDisks e hosts não suportados.
- A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade de licenciamento. Para obter mais informações, consulte Dados de Licenciamento da Citrix.

### Introdução

Este artigo se aplica à instalação de componentes em máquinas com sistemas operacionais Windows. Para obter informações sobre VDAs para sistemas operacionais Linux, consulte Agentes de Entrega Virtual Linux.

Este artigo descreve como emitir comandos de instalação do produto. Antes de iniciar qualquer instalação, revise Preparar para instalar. Esse artigo inclui descrições dos instaladores disponíveis.

Para ver o progresso da execução do comando e os valores de retorno, você deve ser o administrador original ou usar **Executar como administrador**. Para obter mais informações, consulte a documentação de comando da Microsoft.

Como complemento ao uso direto dos comandos de instalação, scripts de exemplo são fornecidos no ISO do produto que instalam, atualizam ou removem VDAs em máquinas no Active Directory. Para obter detalhes, consulte Instalar VDAs usando scripts.

Se você tentar instalar ou atualizar em uma versão do sistema operacional Windows que não seja compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem o guiará para informações sobre suas opções. Consulte Sistemas operacionais anteriores.

Para obter informações sobre como a Citrix relata os resultados das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.

### Usar o instalador completo do produto

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

1. Baixe o pacote do produto da Citrix. As credenciais da conta Citrix são necessárias para acessar o site de download.
2. Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.
3. Faça logon no servidor onde você está instalando os componentes, usando uma conta de administrador local.
4. Insira o DVD na unidade ou monte o arquivo ISO.
5. No diretório `\x64\XenDesktop Setup` da mídia, execute o comando apropriado.

   **Para instalar componentes principais:** Execute `XenDesktopServerSetup.exe`, com as opções listadas em Opções de linha de comando para instalar componentes principais.

   **Para instalar um VDA:** Execute `XenDesktopVDASetup.exe` com as opções listadas em Opções de linha de comando para instalar um VDA.

   **Para instalar o StoreFront:** Execute `CitrixStoreFront-x64.exe` na pasta `x64 > StoreFront` na mídia de instalação.

   **Para instalar o Universal Print Server:** Siga as orientações em Opções de linha de comando para instalar um Universal Print Server.

   **Para instalar o Federated Authentication Service:** A Citrix recomenda usar a interface gráfica.

   **Para instalar o Session Recording:** Siga as orientações em Session Recording.

   **Para instalar o Workspace Environment Management:** Siga as orientações em Workspace Environment Management.

**Para instalar o Secure Private Access:** Execute `XenDesktopSPASetup.exe` na pasta de instalação `x64 > XenDesktop` na mídia de instalação. Siga as orientações em Opções de linha de comando para instalar um Secure Private Access.

### Opções de linha de comando para instalar componentes principais

As seguintes opções de parâmetro são válidas ao instalar componentes principais com o comando `XenDesktopServerSetup.exe`. Para mais detalhes sobre as opções, consulte Instalar componentes principais.

**Observação:**

- Não use `/exclude` ao usar opções de linha de comando para instalar componentes principais.
- Se você atualizar um componente usando `/components`, outros componentes também poderão ser atualizados. Isso é para evitar possíveis problemas de compatibilidade entre diferentes componentes.
- Se você deseja atualizar apenas um componente, use o instalador individual desse componente. Consulte Atualizar uma implantação.

- **/ceipoptin** *ceipoptin* (e outras opções).

  Habilita a coleta de dados do Call Home e dados do Programa de Melhoria da Experiência do Cliente (CEIP). Os valores válidos são:

  - `DIAGNOSTIC`: Escolha este valor para permitir que o Citrix Licensing colete dados do Call Home.
  - `ANONYMOUS`: Escolha este valor para permitir que o Citrix Licensing colete dados CEIP não identificados (que não identificam usuários).
  - `NONE`: Escolha este valor para desabilitar a coleta de dados CEIP pelo Citrix Licensing.

  Para obter mais informações sobre a coleta de dados do Call Home, consulte Citrix Licensing Call Home.

  Para obter mais detalhes sobre a coleta de dados CEIP, consulte Citrix Licensing Customer Experience Improvement Program.

  Para obter mais detalhes sobre os dados CEIP, consulte Citrix Licensing CEIP data elements.

Para obter mais detalhes sobre os dados de licenciamento do License Server, consulte Citrix Licensing Data.

- **/components** *componente ...*

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

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server
  - `SECUREPRIVATEACCESS`: Secure Private Access

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

  (Em versões anteriores a 2003, os valores válidos incluíam `STOREFRONT`. Para a versão 2003 e posterior, use o comando de instalação dedicado do StoreFront mencionado em 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 de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall de terceiros ou nenhum firewall, deverá abrir as portas manualmente.

- **/desabilitarmétricasdeexperiência**

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

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

  Exibe a ajuda do comando.

- **/ignore_hw_check_failure**

  Permite que a instalação ou atualização do Delivery Controller continue, mesmo que as verificações de hardware falhem (por exemplo, devido a RAM insuficiente). Para obter mais informações, consulte Verificação de hardware.

- **/ignore_site_test_failure**

Válido apenas durante a atualização do Controller. Geralmente, quaisquer falhas de teste de site são ignoradas e a atualização prossegue. Se omitido (ou definido como falso), qualquer falha de teste de site faz com que o instalador falhe, sem realizar a atualização. Padrão = false

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

- **/installdir** ***diretório***

  Diretório vazio existente onde os componentes serão instalados. Padrão = `c:\Program Files\Citrix`.

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

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

- **/no_remote_assistance**

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

- **/semreinicialização**

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

- **/semretomar**

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

- **/nosql** (opção)

  Impede a instalação do Microsoft SQL Server Express no servidor onde você está instalando o Controller. Se esta opção for omitida, o SQL Server Express será instalado para ser usado como banco de dados do site.

  Esta opção não afeta a instalação do SQL Server Express LocalDB usado para o Cache de Host Local.

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

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

- **/remover**

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

- **/removertudo**

  Remove todos os componentes principais instalados.

- **/SKIPHDXDRIVERCHECK**

  Ignora a verificação dos drivers HDX™ para o Meta-instalador do VDA.

- **/enviarmetricasdeexperiencia**

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

- **dirtemp** *diretório*

  Diretório que contém arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

- **/XenApp**

  Instala o Citrix Virtual Apps. Se esta opção for omitida, o Citrix Virtual Apps and Desktops™ será instalado.

### Exemplos de instalação de componentes principais

O comando a seguir instala um Delivery Controller™, Studio, Citrix Licensing e SQL Server Express em um servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

O comando a seguir instala um Citrix Virtual Apps™ Controller, Studio e SQL Server Express no servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

`\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall`

O comando a seguir instala um Delivery Controller, Secure Private Access e SQL Server Express em um servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

`\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

### Usar um instalador VDA autônomo

As credenciais da conta Citrix são necessárias para acessar o site de download. Você deve ter privilégios administrativos elevados antes de iniciar a instalação ou usar **Executar como administrador**.

1. Baixe o pacote apropriado da Citrix:
   - Agente de Entrega Virtual de SO multi-sessão: `VDAServerSetup_xxxx.exe`
   - Agente de Entrega Virtual de SO de sessão única: `VDAWorkstationSetup_xxxx.exe`
   - Agente de Entrega Virtual de Serviços Principais de SO de sessão única: `VDAWorkstationCoreSetup_xxxx.exe`
2. Primeiro, extraia os arquivos do pacote para um diretório existente e, em seguida, execute o comando de instalação, ou simplesmente execute o pacote.

   Para extrair os arquivos antes de instalá-los, use `/extract` com o caminho absoluto, por exemplo `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. O diretório deve existir. Caso contrário, a extração falha. Em seguida, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

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

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

Se você estiver familiarizado com o instalador completo do produto:

- Execute o instalador autônomo `VDAServerSetup.exe` ou `VDAWorkstationSetup.exe` como se fosse o comando `XenDesktopVdaSetup.exe` em tudo, exceto em seu nome.
- O instalador `VDAWorkstationCoreSetup.exe` é diferente, porque ele suporta um subconjunto das opções disponíveis para os outros instaladores.

### Opções de linha de comando para instalar um VDA

As seguintes opções são válidas com um ou mais dos seguintes comandos (instaladores): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` e `VDAWorkstationCoreSetup_xxxx.exe`.

Para mais detalhes sobre as opções, consulte Instalar VDAs.

- **/componentes** *componente*\[,*componente*\]

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

  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: aplicativo Citrix Workspace™ para Windows

  Para instalar o VDA e o aplicativo Citrix Workspace para Windows, especifique `/components vda,plugins` ou não especifique nenhum componente. Se nenhum componente for especificado, apenas o VDA será instalado por padrão.

  Para instalar apenas o VDA e excluir a instalação do aplicativo Citrix Workspace, especifique `/components vda`.

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

- **/controllers** "*controlador* \[*controlador*\]"

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

- **/desabilitarmétricasdeexperiência**

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

- **/enable_hdx_ports**

  Abre as portas no firewall do Windows exigidas pelo VDA e pelos recursos habilitados (exceto Assistência Remota do Windows), se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

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

- **/enable_hdx_udp_ports**

  Abre as portas UDP no firewall do Windows que o transporte adaptativo HDX usa, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

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

- **/enable_hdx_tls_dtls**

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

- **/enable_real_time_transport**

  Habilita ou desabilita o uso de UDP para pacotes de áudio (RealTime Audio Transport para áudio). Habilitar este recurso pode melhorar o desempenho do áudio. Inclua a opção `/enable_hdx_ports` se você quiser que as portas UDP sejam abertas automaticamente quando o Serviço de Firewall do Windows for detectado.

- **/enable_remote_assistance**

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

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

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

Se a instalação/atualização for concluída com êxito:

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

Para obter detalhes, consulte Restaurar em caso de falha na instalação ou atualização.

- **/enable_ss_ports**

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

- **/exclude** "*componente*"\[,"*componente*"\]

  Impede a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas simples. Por exemplo, instalar ou atualizar um VDA em uma imagem que não é gerenciada pelo MCS não requer o componente Machine Identity Service. Os valores válidos são os seguintes:

| SO MULTISSESSÃO | SO DE SESSÃO ÚNICA | SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA |
|---|---|---|
| `Citrix App Protection Component` | `Citrix App Protection Component` | `Citrix App Protection Component` |
| `Citrix Authentication Identity Assertion VDA Plug-in` | `Citrix Authentication Identity Assertion VDA Plug-in` | `Citrix Authentication Identity Assertion VDA Plug-in` |
| `Citrix Backup and Restore` | `Citrix Backup and Restore` | |
| `Citrix Browser Content Redirection` | `Citrix Browser Content Redirection` | `Citrix Browser Content Redirection` |
| `Citrix HyperV Filter Driver` | `Citrix HyperV Filter Driver` | |
| `Citrix MCS IODriver` | `Citrix MCS IODriver` | |

| SO MULTISSESSÃO | SO DE SESSÃO ÚNICA | SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA |
|---|---|---|
| Citrix Personalization for App-V - VDA | Citrix Personalization for App-V - VDA | Citrix Personalization for App-V - VDA |
| Citrix Profile Management | Citrix Profile Management | |
| Citrix Profile Management WMI Plug-in | Citrix Profile Management WMI Plug-in | |
| Citrix Rendezvous V2 | Citrix Rendezvous V2 | |
| Citrix Telemetry Service | Citrix Telemetry Service | Citrix Telemetry Service |
| Citrix Universal Print Client | Citrix Universal Print Client | Citrix Universal Print Client |
| Citrix Vda Log Capture Service | Citrix Vda Log Capture Service | Citrix Vda Log Capture Service |
| Citrix VDA Upgrade Agent | Citrix VDA Upgrade Agent | |
| CSE Component | CSE Component | CSE Component |
| Director VDA Plug-in | Director VDA Plug-in | Director VDA Plug-in |
| Machine Identity Service | Machine Identity Service | |
| Machine Management Provider | Machine Management Provider | Machine Management Provider |
| | User Personalization Layer | |
| VDA Monitor Plug-in | VDA Monitor Plug-in | VDA Monitor Plug-in |
| VDA WMI Proxy Plug-in | VDA WMI Proxy Plug-in | VDA WMI Proxy Plug-in |

Excluir o Citrix Profile Management da instalação (`/exclude "Citrix Profile Management"`) afeta o monitoramento e a solução de problemas de VDAs com o Citrix Director. Nas páginas **Detalhes do usuário** e **EndPoint**, o painel Personalização e o painel Duração do logon falham. Nas páginas **Painel** e **Tendências**, o painel Duração Média do Logon exibe dados apenas para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Serviço de Gerenciamento de Perfil da Citrix. A habilitação do Serviço de Gerenciamento de Perfil da Citrix não é obrigatória.

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

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

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

  Exibe a ajuda do comando.

- **/includeadditional** "*componente*"\[,"*componente*"\]

  Inclui a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas simples. Esta opção pode ser útil ao criar uma implantação de Acesso Remoto a PC e desejar instalar outros componentes que não 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 for App-V - VDA` | `Citrix Personalization for App-V - VDA` |
| `Citrix Profile Management` | `Citrix Profile Management` |
| `Citrix Profile Management WMI Plug-in` | `Citrix Profile Management WMI Plug-in` |
| `Citrix Rendezvous V2` | `Citrix Rendezvous V2` |

| SO MULTISSESSÃO | SO DE SESSÃO ÚNICA |
| --- | --- |
| `Citrix VDA Upgrade Agent` | `Citrix VDA Upgrade Agent` |
| `Citrix Web Socket Vda Registration Tool` | `Citrix Web Socket Vda Registration Tool` |
| `Machine Identity Service` | `Machine Identity Service` |
| | `User Personalization Layer` |

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

- **/installdir** *diretório*

  Diretório vazio existente onde os componentes serão instalados. Padrão = `c:\Program Files\Citrix`.

- **/install_mcsio_driver**

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

- **/logpath** *caminho*

  Local do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = "`%TEMP%\Citrix\XenDesktop Installer`"

  Esta opção não está disponível na interface gráfica.

- **/imagem mestre**

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

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

- **/imagem mestre mcs**

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

- **/imagem mestre pvs**

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

- **/websockettoken** *TokenDeWebSocket*

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

- **/no_mediafoundation_ack**

  Reconhece que o Microsoft Media Foundation não está instalado e que vários recursos multimídia HDX não serão instalados e não funcionarão. Se esta opção for omitida e o Media Foundation não estiver instalado, a instalação do VDA será encerrada, pois as pré-condições não foram atendidas. A maioria das edições do Windows suportadas já vem com o Media Foundation instalado, exceto as edições N. Se você habilitar os Recursos do Windows > Recursos de Mídia *manualmente*, a chave do registro procurada pelo Citrix Meta Installer pode não ter um valor definido. Verifique a chave do registro `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` antes de iniciar o processo de instalação para confirmar que o valor existe e não está vazio.

- **/semexperiênciadedesktop**

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

  Válido apenas ao instalar um VDA para SO multi-sessão. Impede a ativação do recurso Enhanced Desktop Experience. Este recurso também é controlado pela configuração de política Citrix Enhanced Desktop Experience.

- **/semreinicialização**

  Impede uma reinicialização após a instalação. O VDA não pode ser usado antes de uma reinicialização.

- **/semretomar**

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

- **/máquinafísica**

Use este argumento junto com `/remotepc` para a instalação do RemotePC. Caso contrário, o VDA pode não se comportar como esperado em certos cenários de usuário.

- **/númerodaporta** *porta*

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

- **/proxyconfig** "*endereço ou caminho do arquivo PAC*"

  Se você planeja usar o protocolo Rendezvous V2 com um serviço como o Gateway Service em seu ambiente e tem um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Apenas proxies HTTP são suportados. O endereço ou caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para detalhes do recurso, consulte protocolo Rendezvous.

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

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

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

- **/reconfigurar**

  Personaliza as configurações do VDA configuradas anteriormente quando usado com as opções `/portnumber`, `/controllers` ou `/enable_hdx_ports`. Se você especificar esta opção sem também especificar a opção `/quiet`, a interface gráfica para personalizar o VDA será iniciada.

- **/pcremoto**

  Válido apenas para implantações de Acesso Remoto a PC (SO de sessão única) ou conexões intermediadas (SO de multi-sessão). Exclui a instalação de quaisquer componentes adicionais (consulte as listas de componentes com as opções `/exclude` e `/includeadditional`).

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

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

- **/remover**

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

- **/remove_appdisk_ack**

  Autoriza o instalador do VDA a desinstalar o plug-in AppDisks™ VDA, se estiver instalado.

- **/remove_pvd_ack**

  Autoriza o instalador do VDA a desinstalar o Personal vDisk, se estiver instalado.

- **/removertudo**

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

- **/REMOVEALLWITHCWA**

  Remove o CWA junto com o VDA.

- **/enviarmetricasdeexperiencia**

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

- **servidorvdi**

  Instala um VDA para SO de sessão única em uma máquina Windows multissessão compatível. Omita esta opção ao instalar um VDA para SO multissessão em uma máquina Windows multissessão.

  Antes de usar esta opção, consulte Server VDI.

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

- **local_guid** *guid*

  Identificador Globalmente Único da Unidade Organizacional (OU) do Active Directory do site. Isso associa um desktop virtual a um site quando você está usando o Active Directory para descoberta (a atualização automática é o método de descoberta recomendado e padrão). O GUID do site é uma propriedade do site exibida no Studio. Não especifique as opções `/site_guid` e `/controllers`.

- **dirtemp** *diretório*

  Diretório para armazenar arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

Esta opção não está disponível na interface gráfica.

- **máquinavirtual**

  Válido apenas ao instalar um VDA em uma VM. Substitui a detecção pelo instalador de uma máquina física, onde as informações do BIOS passadas para as VMs as fazem parecer máquinas físicas.

  Esta opção não está disponível na interface gráfica.

- **xendesktopnuvem**

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

### Exemplos de instalação de um VDA

**Instalar um VDA com o instalador completo do produto:**

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

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional "user personalization layer" /mastermcsimage /enable_remote_assistance
```

**Instalar um VDA de SO de sessão única com o instalador autônomo VDAWorkstationCoreSetup:**

O comando a seguir instala um VDA de Serviços Principais em um SO de sessão única para uso em uma implantação de Acesso Remoto a PC ou VDI. O aplicativo Citrix Workspace e outros serviços não essenciais não são instalados. O endereço de um Controller é especificado, e as portas no Serviço de Firewall do Windows serão abertas automaticamente. O administrador manipular os reinícios.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

### Personalizar um VDA

Após instalar um VDA, você pode personalizar várias configurações. No diretório `\x64\XenDesktop Setup` na mídia do produto, execute `XenDesktopVdaSetup.exe`, usando uma ou mais das seguintes opções, que são descritas em Opções de linha de comando para instalar um VDA.

- `/reconfigure` (obrigatório ao personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

### Solucionar problemas de VDAs

- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Após a instalação de um VDA, ele não pode entregar aplicativos ou um desktop aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

### Opções de linha de comando para instalar um Universal Print Server

A seguinte opção é válida com o comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

Quando esta opção não é especificada, o instalador exibe a página **Firewall** da interface gráfica. Selecione **Automaticamente** para que o instalador adicione automaticamente as regras de firewall do Windows, ou **Manualmente** para permitir que o administrador configure o firewall manualmente.

Após instalar o software em seus servidores de impressão, configure o Universal Print Server usando as orientações em Provisionar impressoras.

### Opções de linha de comando para instalar um Secure Private Access

As seguintes opções são válidas com:

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

- **/enable_spa_ports**

  Abre as portas no firewall do Windows exigidas pelo Secure Private Access, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

- **/sem SQL**

  Impede a instalação do Microsoft SQL Server Express no servidor onde você está instalando o Secure Private Access. Se esta opção for omitida, o SQL Server Express será instalado para ser usado como o banco de dados do site.

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

  Exibe a ajuda do comando

- **/semreinicialização**

  Impede uma reinicialização após a instalação. O Secure Private Access não pode ser usado antes de uma reinicialização.

- **/quiet ou /passive**

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

- **/remover**

  Remove o Secure Private Access.

Para obter mais detalhes sobre as opções, consulte instalador do Secure Private Access.

### Mais informações

Para obter informações sobre como a Citrix relata o resultado das instalações de componentes, consulte códigos de retorno de instalação da Citrix.

# Instalar VDAs

**Importante:**

- Se você estiver atualizando e sua versão atual tiver o software Personal vDisk ou AppDisks instalado, consulte Removendo PvD, AppDisks e hosts não suportados.
- Os binários distribuídos pela Citrix® agora são assinados. Binários assinados indicam que são validados por certificados gerados pela Citrix ou por certificados autênticos de terceiros.

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

Antes de iniciar uma instalação, revise Preparar para instalar e conclua todas as tarefas de preparação.

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

Este artigo descreve a sequência do assistente de instalação ao instalar um VDA. Equivalentes de linha de comando são fornecidos. Para obter detalhes, consulte Instalar usando a linha de comando.

## Etapa 1. Baixe o software do produto e inicie o assistente

Se você estiver usando o instalador completo do produto:

1. Se você ainda não baixou o ISO do produto:
   - Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.
   - Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.
2. Use uma conta de administrador local na imagem ou máquina onde você está instalando o VDA. Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não iniciar automaticamente, clique duas vezes no aplicativo **AutoSelect** na unidade montada.

   O assistente de instalação é iniciado.

Se você estiver usando um pacote autônomo:

1. Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o pacote apropriado:
   - `VDAServerSetup_2402.exe`: VDA de SO multissessão *versão*
   - `VDAWorkstationSetup_2402.exe`: VDA de SO de sessão única *versão*
   - `VDAWorkstationCoreSetup_2402.exe`: VDA de Serviços Principais de SO de sessão única *versão*
2. Clique com o botão direito do mouse no pacote e escolha **Executar como administrador.**

   O assistente de instalação é iniciado.

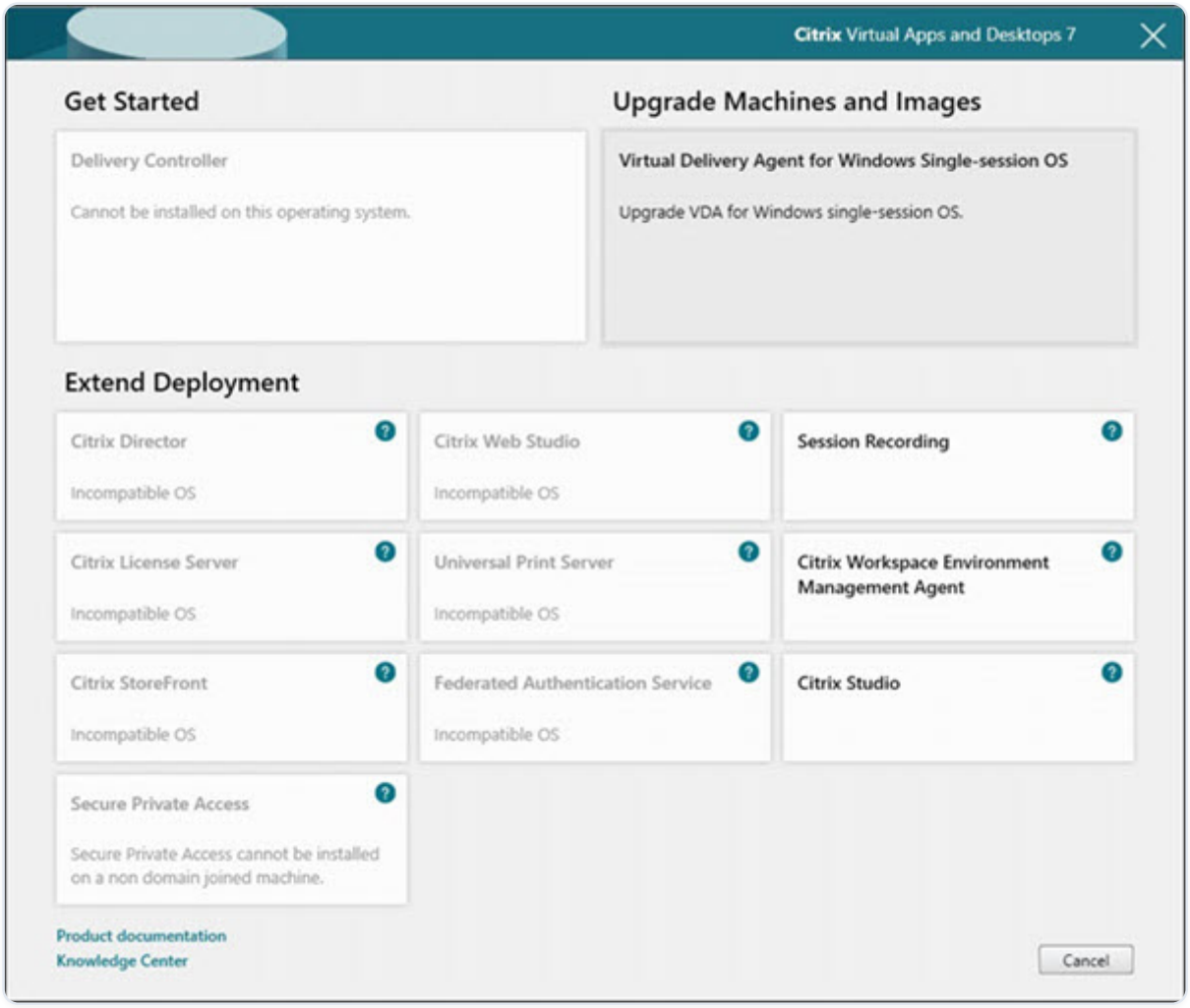
## Etapa 2. Escolha qual produto instalar




Clique em **Iniciar** ao lado do produto a ser instalado: Citrix Virtual Apps ou Citrix Virtual Desktops. (Se a máquina já tiver um componente do Citrix Virtual Apps ou Citrix Virtual Desktops instalado, esta página não aparecerá.)

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

## Etapa 3. Selecione o VDA

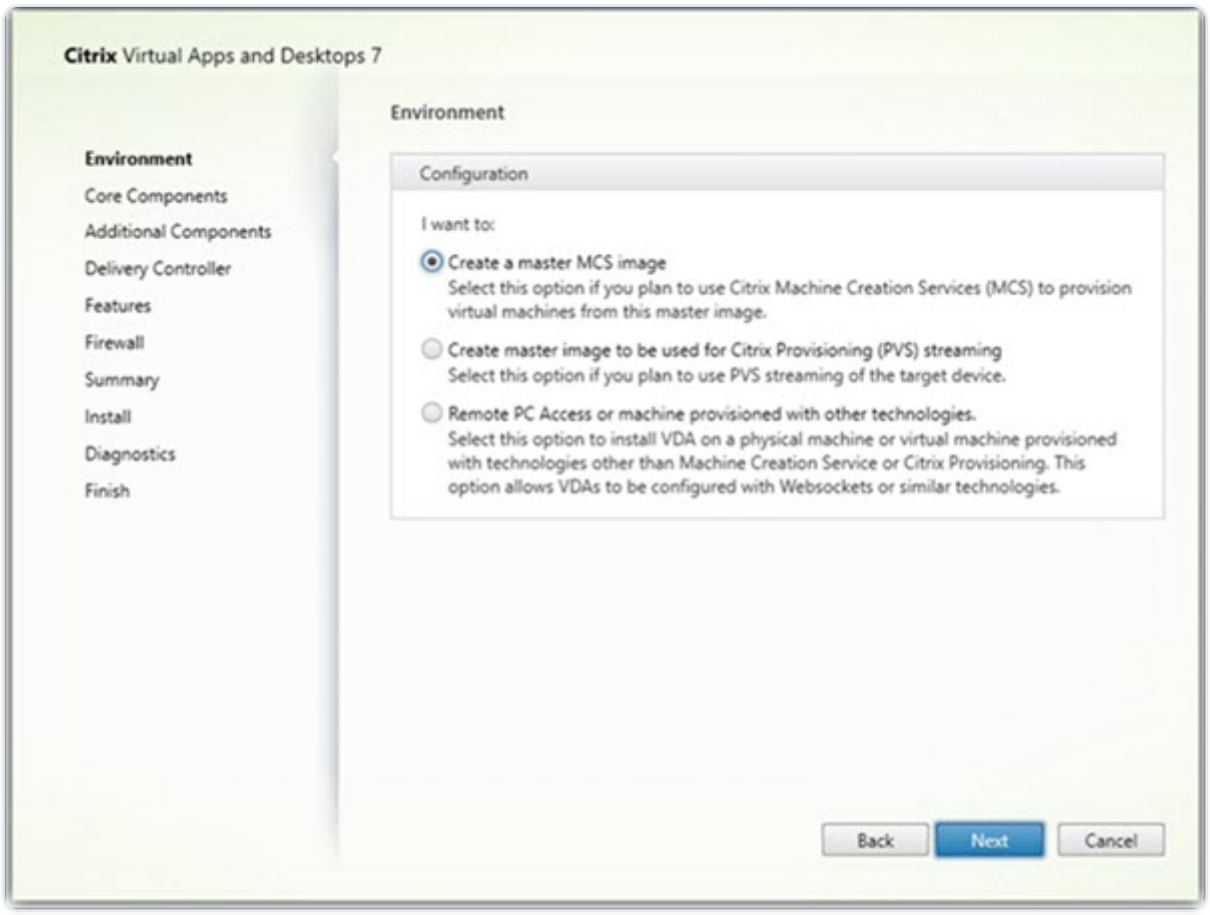



Selecione a entrada **Virtual Delivery Agent**. O instalador sabe se está sendo executado em um SO de sessão única ou multissessão, portanto, oferece apenas o tipo de VDA apropriado.

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

Se você tentar instalar (ou atualizar para) um VDA do Windows em um SO que não seja compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem o guiará para informações sobre as opções.

## Etapa 4. Especifique como o VDA será usado




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

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

Escolha uma das seguintes opções:

- **Criar uma imagem mestre do MCS:** Selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar o Machine Creation Services™ para provisionar VMs. Esta opção instala o Machine Identity Service. Esta é a opção padrão.

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

> **Importante:**

> A mídia de instalação ou imagem ISO deve ser montada localmente. Montar uma imagem ISO de um drive de rede para fins de instalação de software não é suportado.

- **Criar uma imagem mestre usando Citrix Provisioning ou ferramentas de provisionamento de terceiros:** Selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar o Citrix Provisioning ou ferramentas de provisionamento de terceiros (como o Microsoft System Center Configuration Manager) para provisionar VMs.

  Opção de linha de comando: `/masterpvsimage`

- (Aparece apenas em máquinas OS multi-sessão) **Habilitar conexões intermediadas a um servidor:** Selecione esta opção para instalar um VDA em uma máquina física ou virtual que não será usada como imagem para provisionar outras máquinas.

  Opção de linha de comando: `/remotepc`

- (Aparece apenas em máquinas OS de sessão única) **Habilitar Acesso Remoto a PC:** Selecione esta opção para instalar um VDA em uma máquina física para uso com Acesso Remoto a PC.

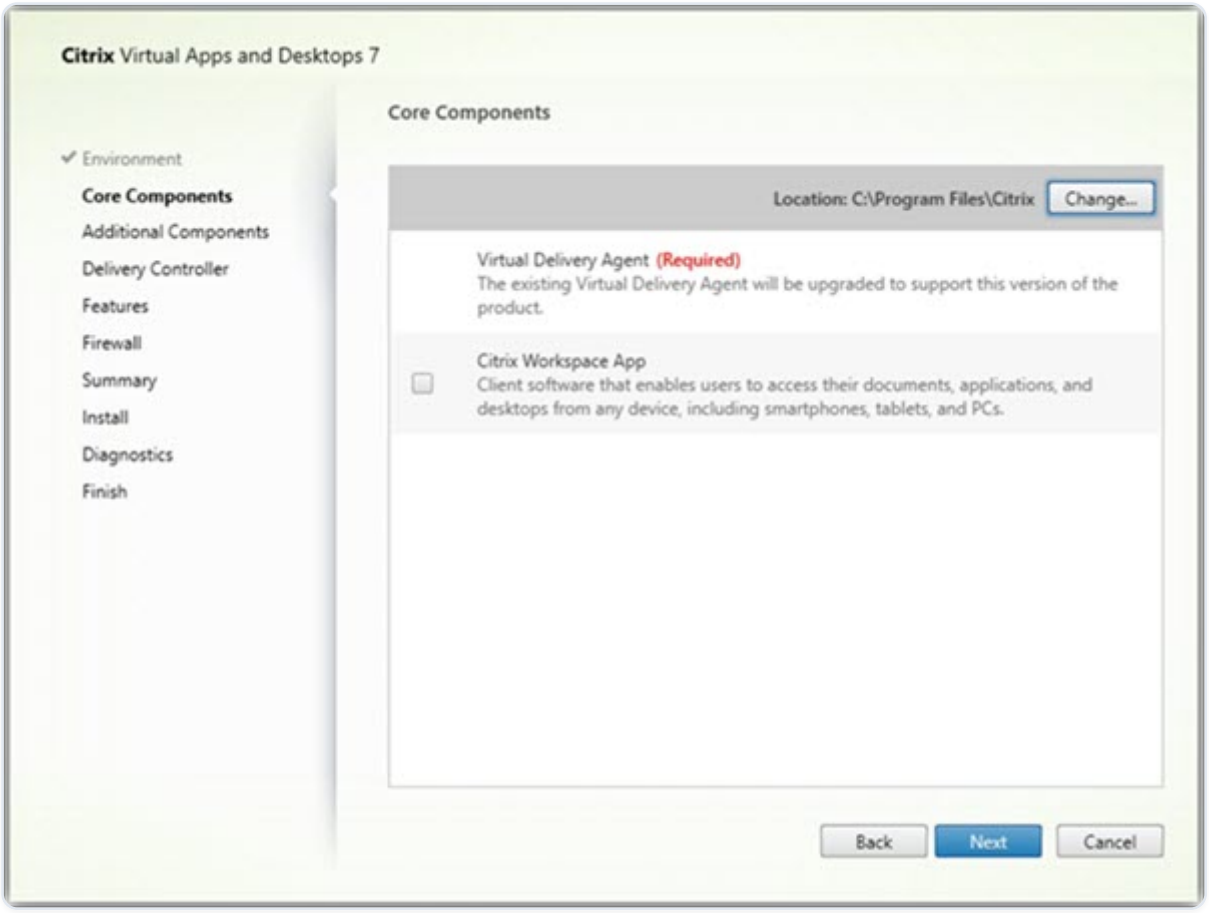
  Opção de linha de comando: `/remotepc`

Clique em **Avançar**.

Esta página não aparece:

- Se você estiver atualizando um VDA
- Se você estiver usando o instalador `VDAWorkstationCoreSetup_2308.exe` , `VDAServerSetup_2308.exe` ou `VDAWorkstationSetup_2308.exe`

## Etapa 5. Selecione os componentes a serem instalados e o local de instalação




Na página **Componentes principais**:

- **Local:** Por padrão, os componentes são instalados em `C:\Program Files\Citrix`. Este padrão é adequado para a maioria das implantações. Se você especificar um local diferente, esse local deve ter permissões `execute` para o serviço de rede.
- **Componentes:** 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, esta caixa de seleção não é exibida.

Clique em **Avançar**.

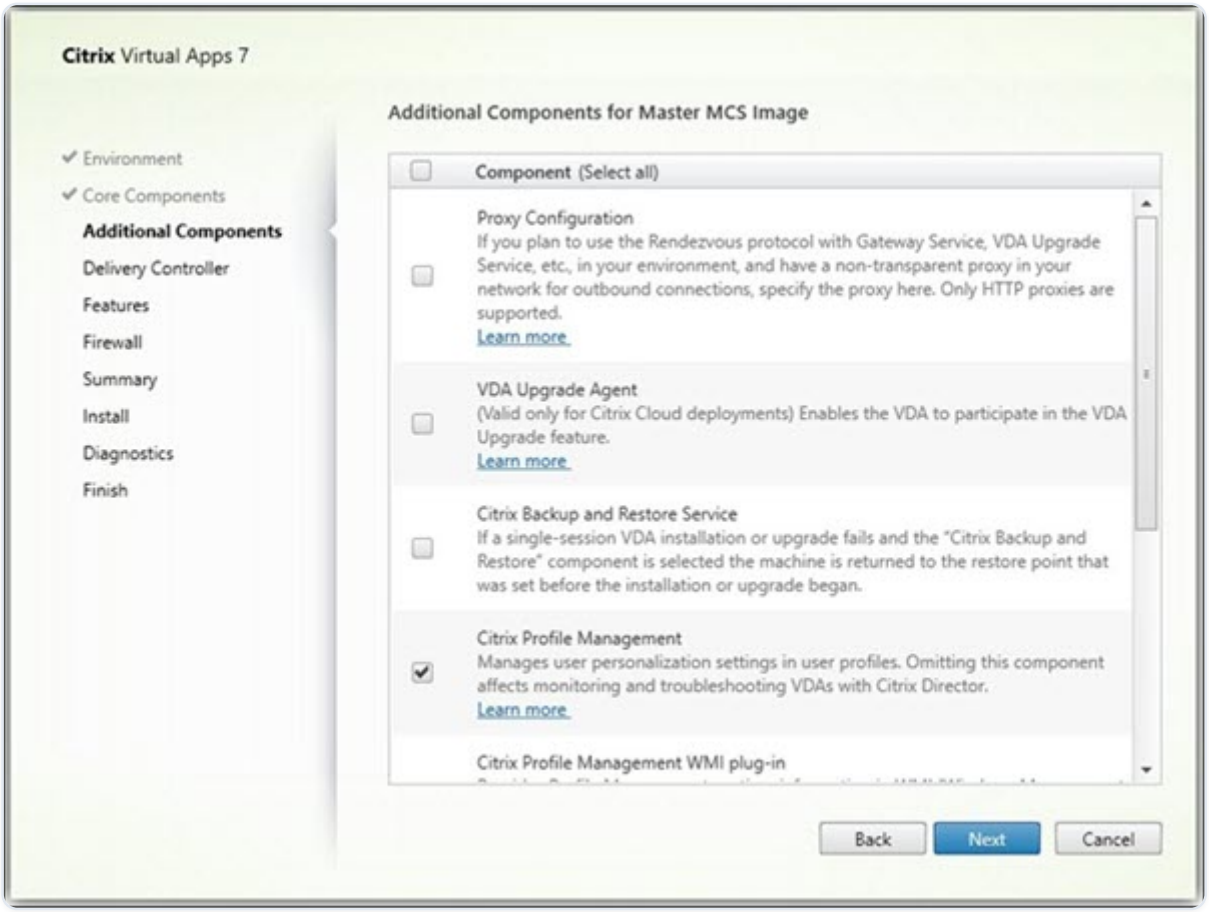
Opções de linha de comando: `/installdir`, `/components vda,plugin` para instalar o VDA e o aplicativo Citrix Workspace para Windows

> **Observação:**

> Você pode optar por instalar, atualizar ou desinstalar o aplicativo Citrix Workspace™ durante uma instalação, atualização ou desinstalação do VDA nos seguintes cenários:

- Durante uma 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 pode 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 uma 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. Instalar componentes adicionais




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

- **/includeadditional** "*componente*"\[,"*componente*"\] ...
- **/exclude** "*componente*"\[,"*componente*"\] ...

A tabela a seguir indica a configuração padrão dos itens nesta página. A configuração padrão depende da opção que você selecionou na página **Ambiente**.

| PÁGINA COMPONENTES ADICIONAIS | PÁGINA AMBIENTE: "IMAGEM MESTRE COM MCS" OU "IMAGEM MESTRE COM CITRIX PROVISIONING" SELECIONADO | PÁGINA AMBIENTE: "HABILITAR CONEXÕES INTERMEDIADAS AO SERVIDOR" (PARA SO MULTI-SESSÃO) OU "ACESSO REMOTO PARA PC" (PARA SO DE SESSÃO ÚNICA) SELECIONADO |
|---|---|---|
| Citrix Personalização para App-V - VDA | Não selecionado | Não selecionado |
| Camada de Personalização do Usuário | Não selecionado | Não exibido porque não é válido para este caso de uso. |
| Citrix Profile Management | Selecionado | Não selecionado |
| Citrix Profile Management WMI Plug-in | Selecionado | Não selecionado |
| Citrix VDA Upgrade Agent | Não selecionado | Não selecionado |
| Citrix Backup e Restauração | Não selecionado | Não selecionado |
| Citrix MCS IODriver | Não selecionado | Não selecionado |
| Citrix Rendezvous V2 | Não selecionado | Não selecionado |

Esta página não aparece se:

- Você está usando o instalador `VDAWorkstationCoreSetup.exe`. Além disso, as opções de linha de comando para os componentes adicionais não são válidas com esse instalador.
- Você está atualizando um VDA e todos os componentes adicionais já estão instalados. Se alguns dos componentes adicionais já estiverem instalados, a página listará apenas os componentes que não estão instalados.

Selecione ou desmarque as seguintes caixas de seleção. (Os componentes podem aparecer em uma ordem diferente no instalador.)

- **Citrix Personalization for App-V:** Instale este componente se você usar aplicativos de pacotes Microsoft App-V. Para obter detalhes, consulte Implantar e entregar aplicativos App-V.

  Opção de linha de comando: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar a instalação do componente, `/exclude "Citrix Personalization for App-V – VDA"` para impedir a instalação do componente.

- **Citrix User Personalization Layer:** Instala o MSI para a camada de personalização do usuário. Para obter detalhes, consulte Camada de personalização do usuário.

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

  Opção de linha de comando: `/includeadditional "User Personalization Layer"` para habilitar a instalação do componente, `/exclude "User Personalization Layer"` para impedir a instalação do componente.

- **Citrix Profile Management:** Este componente gerencia as configurações de personalização do usuário em perfis de usuário. Para obter detalhes, consulte Profile Management.

  Excluir o 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 apenas para máquinas que têm o Profile Management instalado.

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

  Opção de linha de comando: `/includeadditional "Citrix Profile Management"` para habilitar a instalação do componente, `/exclude "Citrix Profile Management"` para impedir a instalação do componente.

- **Plug-in WMI do Citrix Profile Management:** Este plug-in fornece informações de tempo de execução do Profile Management em objetos WMI (Windows Management Instrumentation) (por exemplo, provedor de perfil, tipo de perfil, tamanho e uso do disco). Os objetos WMI fornecem informações de sessão ao Director.

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

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

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

- **Cache de gravação MCSIO para otimização de armazenamento:** Instala o driver Citrix MCS I/O. Para obter mais informações, consulte Armazenamento compartilhado por hipervisores e Configurar cache para dados temporários.

  Opções de linha de comando: `/includeadditional "Citrix MCS IODriver"` para habilitar a instalação do componente, `/exclude "Citrix MCS IODriver"` para impedir a instalação do componente.

- **Configuração de Proxy:** Instale este componente se você planeja usar o protocolo Rendezvous com o Gateway Service, VDA Upgrade Service e assim por diante, em seu ambiente, e você tem um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Apenas proxies HTTP são suportados.

  Se você instalar este componente, especifique o endereço do proxy ou o caminho do arquivo PAC na página **Rendezvous Proxy Configuration**. Para obter detalhes do recurso, consulte protocolo Rendezvous.

  Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para habilitar a instalação do componente, `/exclude "Citrix Rendezvous V2"` para impedir a instalação do componente.

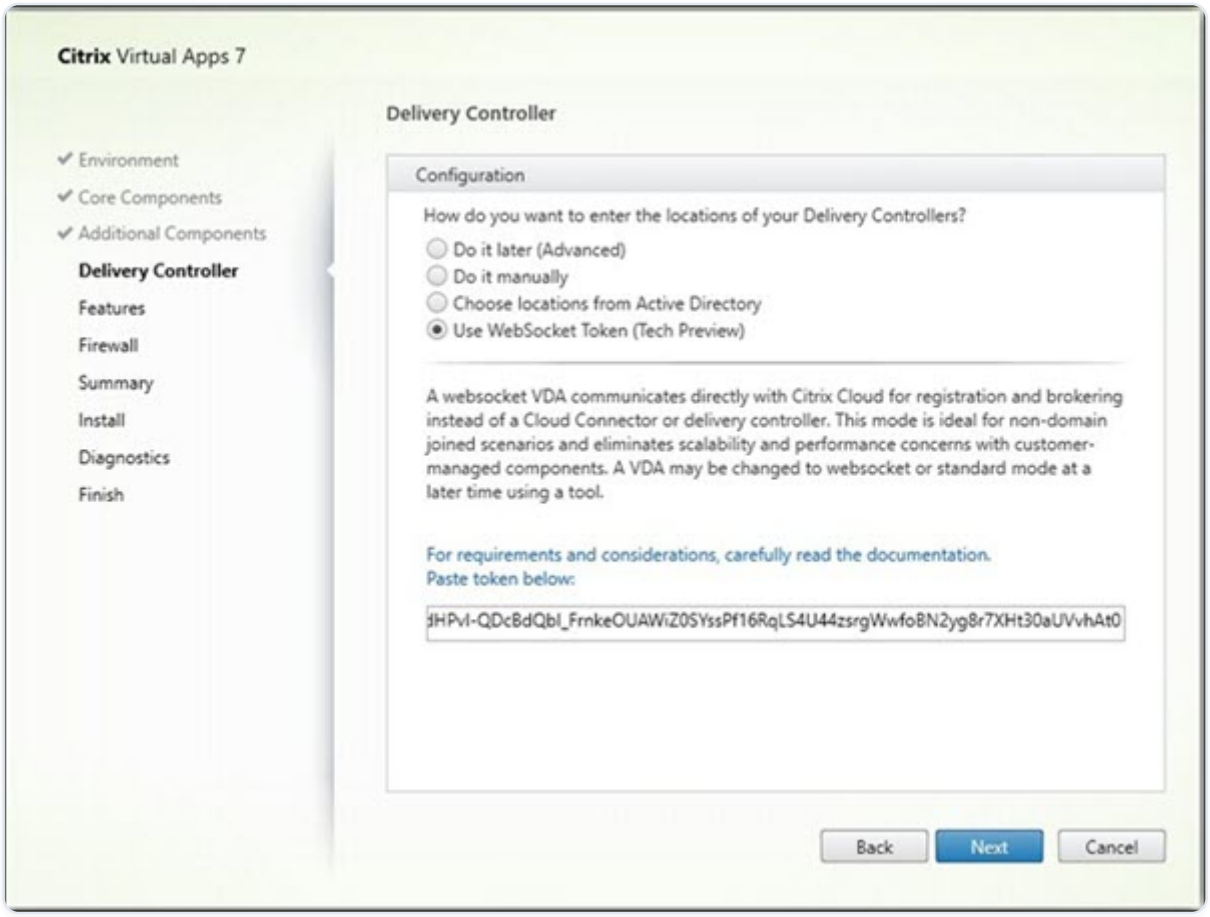
- **Citrix Backup and Restore:** Se uma instalação ou atualização de VDA falhar, este componente pode retornar a máquina a um backup que foi feito antes da instalação ou atualização.

  Certifique-se de que os pré-requisitos da Microsoft sejam atendidos conforme mencionado em Preparar para instalar.

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

> **Observação:**
>
> Se a otimização de armazenamento do MCS estiver ativada, o backup ou a restauração para o sistema operacional de servidor ou desktop Windows pode falhar. Para resolver isso, desative a opção de otimização de armazenamento do MCS no meta instalador.

## Etapa 7. Endereços do Delivery Controller™




Na página **Delivery Controller**, escolha como deseja inserir os endereços dos Controllers instalados. A Citrix recomenda que você especifique os endereços durante a instalação do VDA (**Fazer manualmente**). O VDA não pode se registrar em um Controller até que tenha essas informações. Se um VDA não puder se registrar, os usuários não poderão acessar aplicativos e desktops nesse VDA.

- **Fazer manualmente:** (padrão) Insira o FQDN de um Controller instalado e clique em **Adicionar**. Se você instalou mais Controllers, adicione os endereços deles.
- **Fazer mais tarde (Avançado):** Se você escolher esta opção, o assistente solicitará que você confirme que é isso que deseja fazer antes de continuar. Para especificar endereços mais tarde, você pode executar novamente o instalador ou usar a Política de Grupo da Citrix. O assistente também o lembrará na página **Resumo**.
- **Escolher locais do Active Directory:** Válido apenas quando a máquina está ingressada em um domínio e o usuário é um usuário de domínio.
- **Usar Token WebSocket (Pré-visualização Técnica):** Cria um VDA WebSocket. O WebSocketToken é para o token que é necessário.
- **Deixar o Machine Creation Services fazer isso automaticamente:** Válido apenas ao usar o MCS para provisionar máquinas.

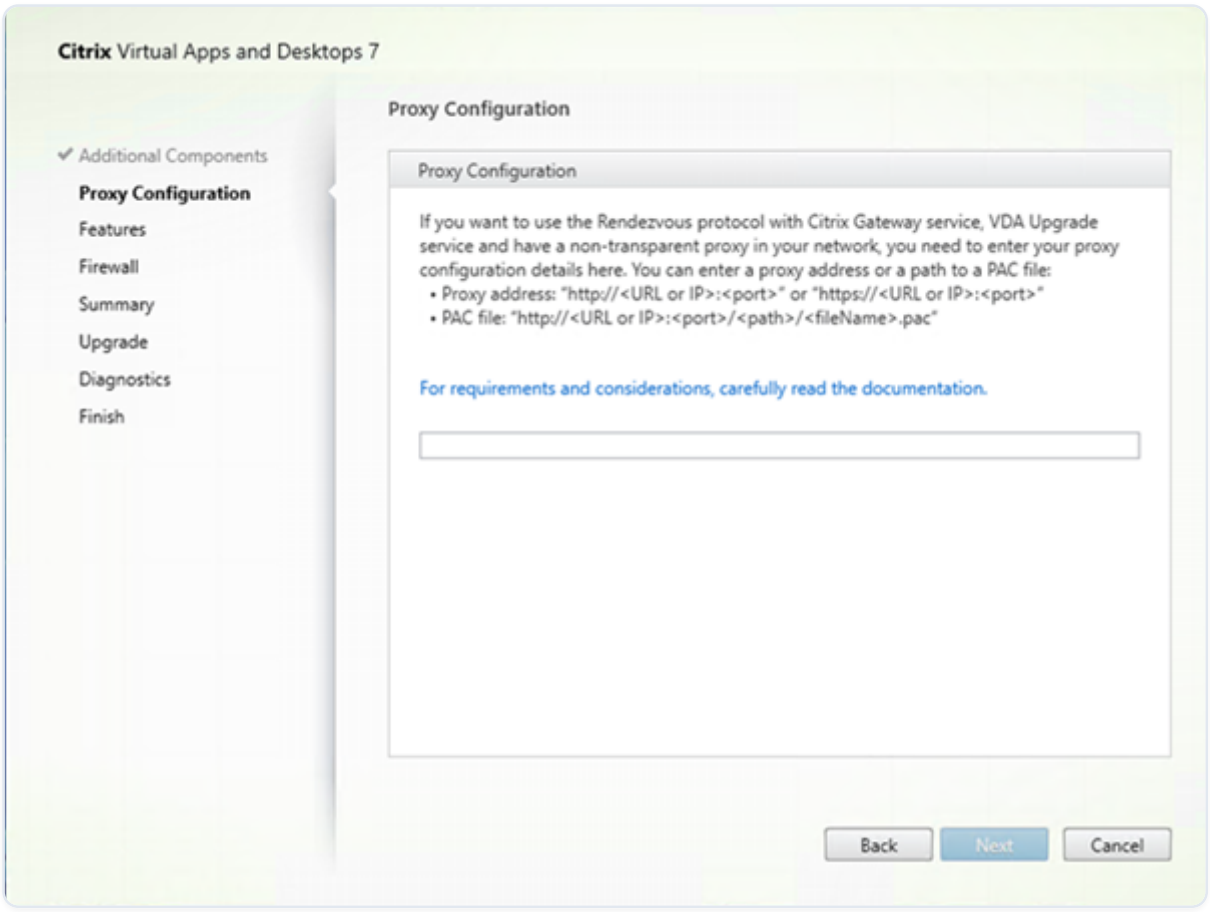
Clique em **Avançar**. Se você selecionou **Fazer mais tarde (Avançado)**, será solicitado a confirmar que especificará os endereços do Controller mais tarde.

Outras considerações:

- O endereço não pode conter caracteres não alfanuméricos.
- Se você especificar endereços durante a instalação do VDA e na Política de Grupo, as configurações da política substituirão as configurações fornecidas durante a instalação.
- O registro bem-sucedido do VDA exige que as portas do firewall usadas para se comunicar com o Controller estejam abertas. Essa ação é habilitada por padrão na página **Firewall** do assistente.
- Depois de especificar os locais do Controller (durante ou após a instalação do VDA), você pode usar o recurso de atualização automática para atualizar os VDAs quando os Controllers forem adicionados ou removidos. Para obter detalhes sobre como os VDAs descobrem e se registram nos Controllers, consulte Registro do VDA.

Opção de linha de comando: `/controllers`

## Etapa 8. Configuração do Proxy



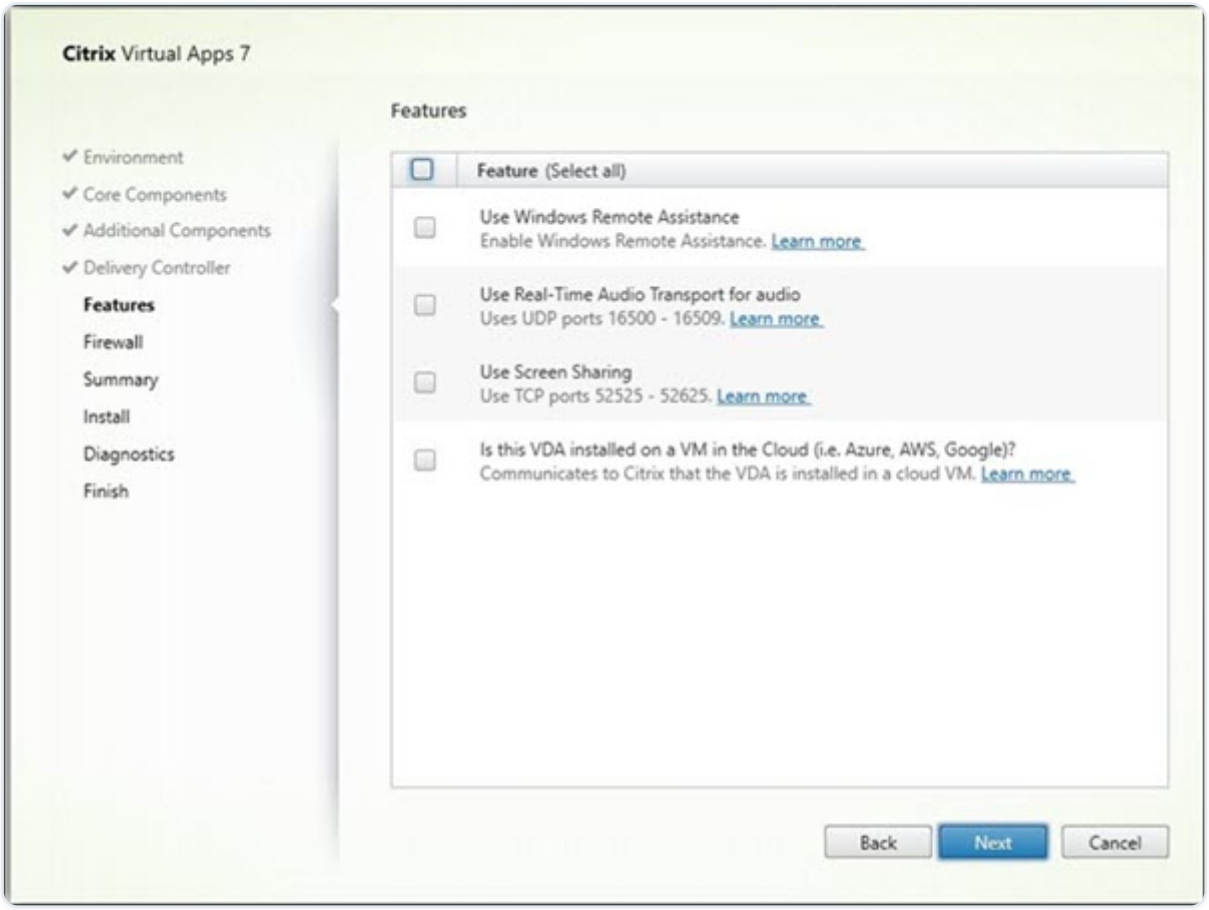

A página **Configuração do Proxy** aparece somente se você ativou a caixa de seleção **Configuração do Proxy** na página **Componentes Adicionais**.

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

O firewall para a porta do proxy deve estar aberto para que o teste de conexão seja bem-sucedido. Se uma conexão não puder ser feita com o proxy, você poderá escolher se deseja continuar com a instalação do VDA.

Opção de linha de comando: `/proxyconfig`

## Etapa 9. Habilitar ou desabilitar recursos




Na página **Recursos**, use as caixas de seleção para habilitar ou desabilitar os recursos que você deseja usar.

- **Usar Assistência Remota do Windows:** Quando este recurso está habilitado, a Assistência Remota do Windows é usada com o recurso de sombreamento de usuário do Director. A Assistência Remota do Windows abre as portas dinâmicas no firewall. (Padrão = desabilitado)

  Opção de linha de comando: `/enable_remote_assistance`

- **Usar Transporte de Áudio em Tempo Real para áudio:** Habilite este recurso se o voice-over-IP for amplamente utilizado em sua rede. O recurso reduz a latência e melhora a resiliência do áudio em redes com perdas. Ele permite que os dados de áudio sejam transmitidos usando RTP sobre transporte UDP. (Padrão = desabilitado)

  Opção de linha de comando: `/enable_real_time_transport`

- **Usar compartilhamento de tela:** Quando habilitado, as portas usadas pelo compartilhamento de tela são abertas no firewall do Windows. (Padrão = desabilitado)

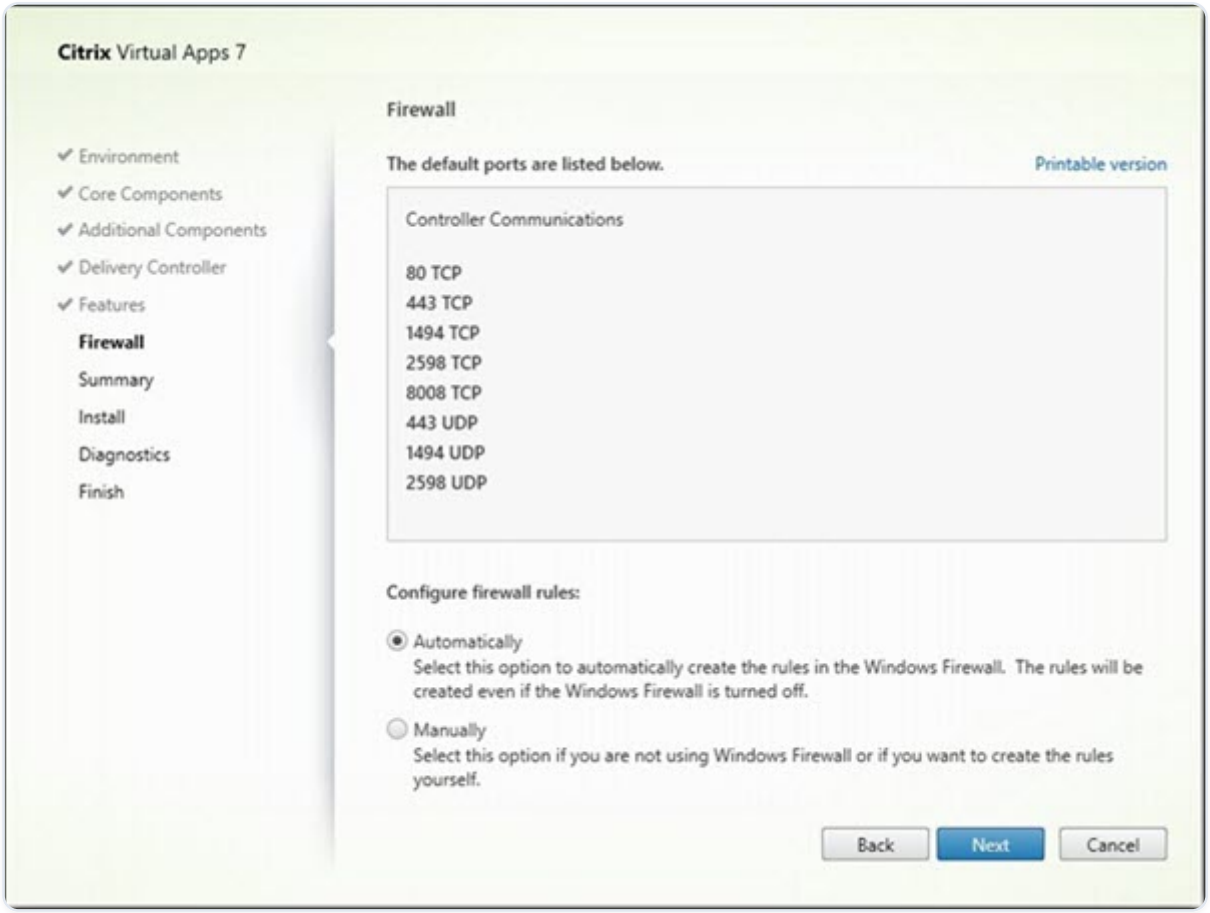
  Opção de linha de comando: `/enable_ss_ports`

- **Este VDA está instalado em uma VM na nuvem:** Esta configuração ajuda a Citrix a identificar corretamente os locais de recursos para implantações de VDA locais e de serviço (Citrix Cloud™) para fins de telemetria. Este recurso não tem impacto na utilização do lado do cliente. Habilite esta configuração se sua implantação usar Citrix DaaS (Padrão = desabilitado).

  Opção de linha de comando: `/xendesktopcloud`

Clique em **Avançar**.

## Etapa 10. Portas do firewall

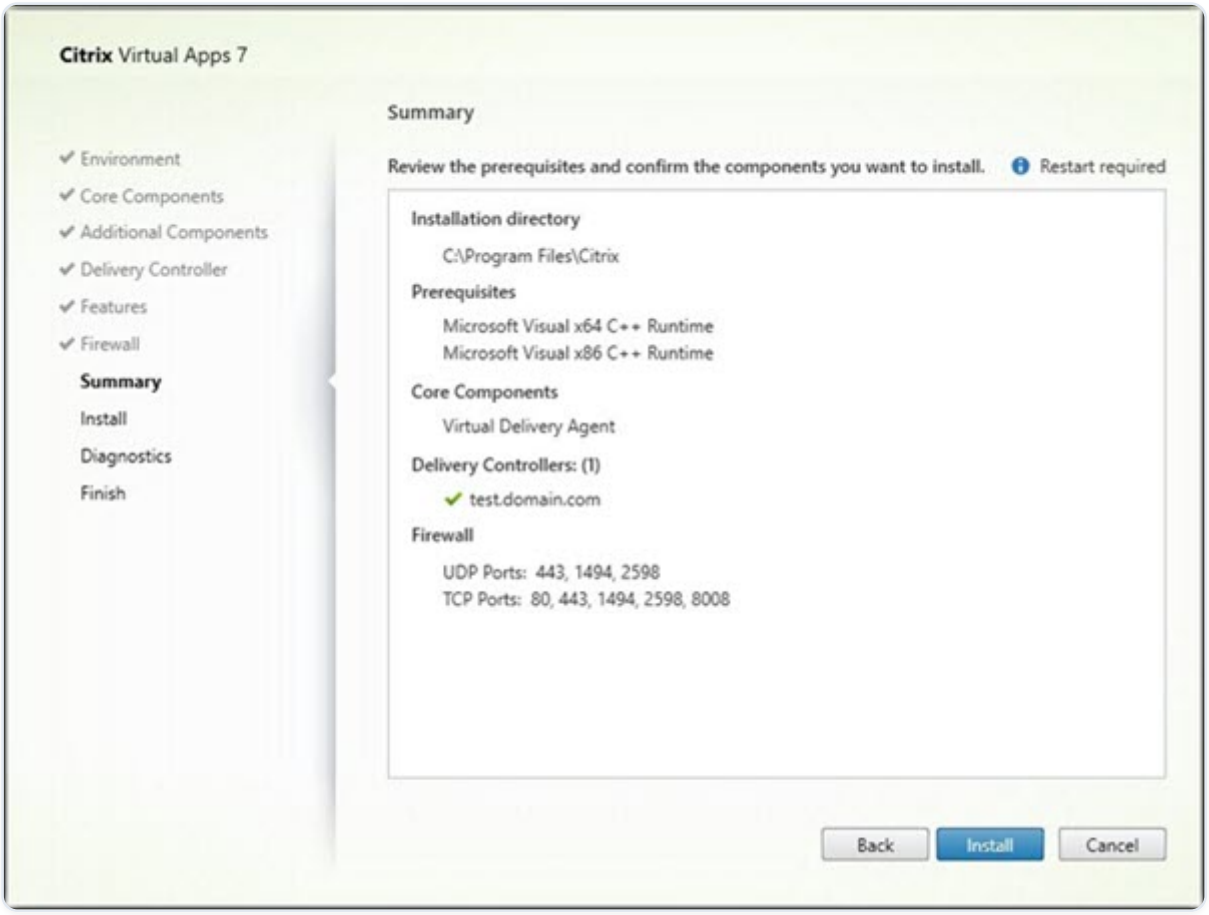



Na página **Firewall**, por padrão, as portas são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja habilitado. Essa configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

Opção de linha de comando: `/enable_hdx_ports`

## Etapa 11. Revisar pré-requisitos e confirmar a instalação

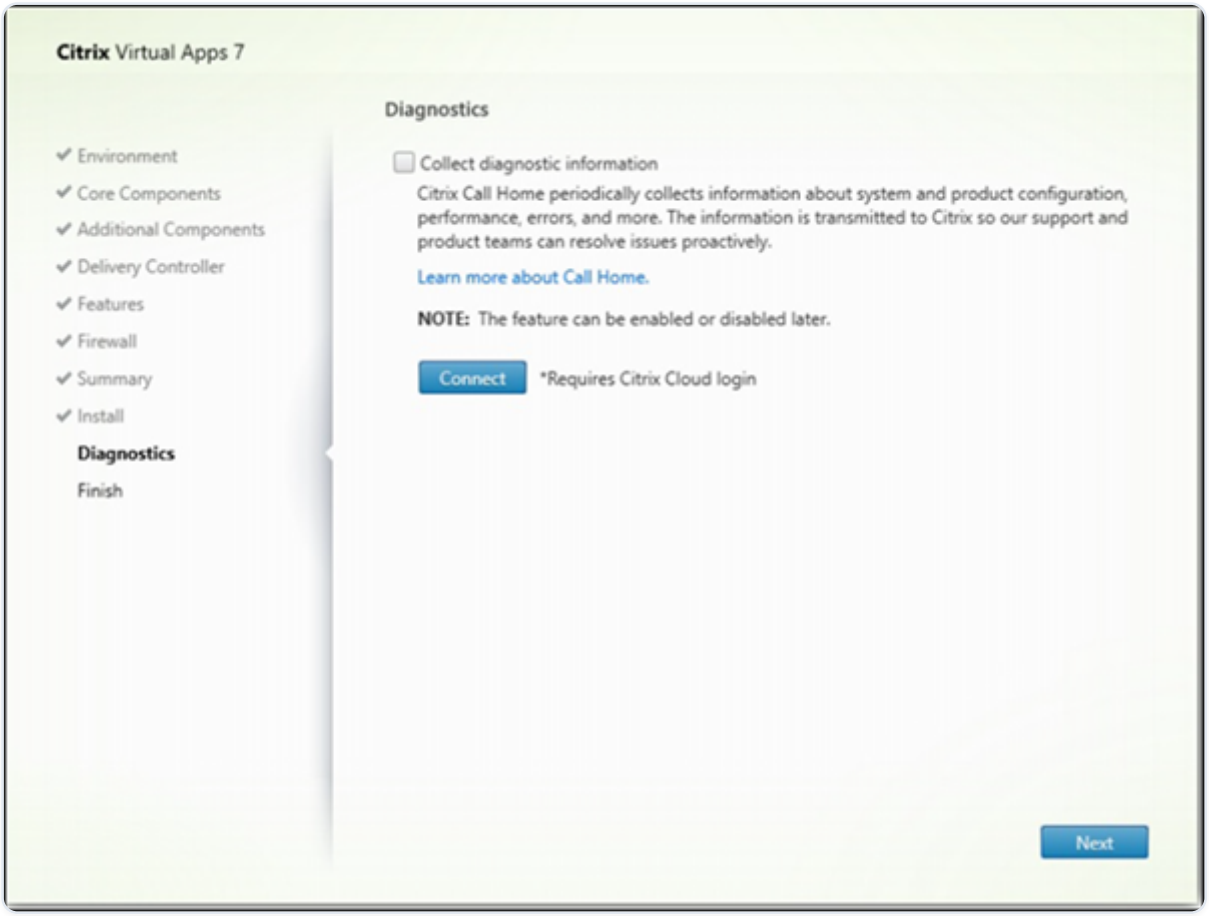



A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções.

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

Se os pré-requisitos ainda não estiverem instalados ou habilitados, a máquina poderá reiniciar uma ou mais vezes. Consulte Preparar para instalar.

## Etapa 12. Diagnóstico



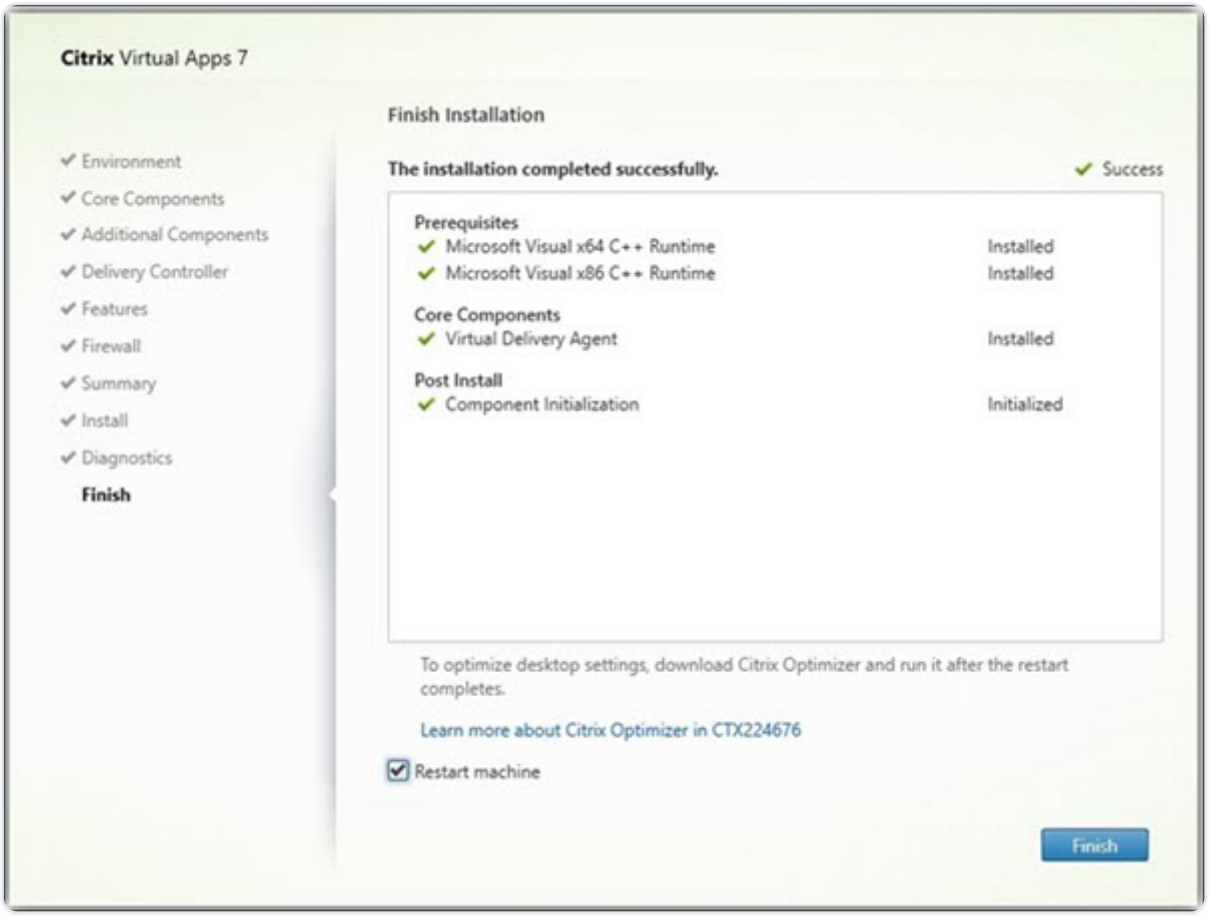

Na página **Diagnóstico**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix.

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

Ao usar o instalador completo do produto, se você clicar em **Conectar** na página **Diagnóstico** sem primeiro selecionar **Coletar informações de diagnóstico**, depois de fechar a caixa de diálogo **Conectar aos Serviços Citrix Insight**, o botão **Avançar** será desabilitado. Você não pode ir para a próxima página. Para reabilitar o botão **Avançar**, selecione e desmarque imediatamente **Coletar informações de diagnóstico**.

Para obter mais informações, consulte Call Home.

## Etapa 13. Concluir esta instalação




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

Clique em **Concluir**. Por padrão, a máquina reinicia automaticamente. Embora você possa desabilitar essa reinicialização automática, o VDA não poderá 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. Consulte:

- Criar um site
- Criar catálogos de máquinas
- Criar grupos de entrega

## Citrix Optimizer

O Citrix Optimizer é uma ferramenta para o sistema operacional Windows que ajuda os administradores Citrix a otimizar VDAs removendo e otimizando vários componentes.

Após instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Consulte CTX224676. O artigo CTX contém o pacote de download, além de instruções sobre como instalar e usar o Citrix Optimizer.

## Personalizar um VDA

Para personalizar um VDA instalado:

1. No recurso do Windows para remover ou alterar programas, selecione **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Em seguida, clique com o botão direito e selecione **Alterar**.
2. Selecione **Personalizar Configurações do Virtual Delivery Agent**. Quando o instalador for iniciado, você pode alterar:
   - Endereços do Controller
   - Porta TCP/IP para registrar com o Controller (padrão = 80)
   - Se deve abrir as portas do Firewall do Windows automaticamente

## Solução de problemas

- Para obter informações sobre como a Citrix relata os resultados das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.
- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou um desktop aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

## Limitação conhecida

Ao usar o aplicativo Citrix Workspace para Windows versão 1912 ou anterior, a sessão é encerrada após um tempo. Esse problema foi corrigido nas versões LTSR e CR mais recentes do aplicativo Citrix Workspace. Para obter mais informações sobre as versões de lançamento

suportadas, consulte Citrix Workspace app para Windows / Citrix Receiver para Windows Long Term Service Releases.

## Configurar o Controle de Acesso do Windows Defender relacionado à Instalação do VDA

Os clientes configuram as definições do Controle de Acesso do Windows Defender (WDAC) para proibir o carregamento de binários não assinados. Os binários não assinados distribuídos pelos instaladores do VDA são, portanto, proibidos, o que restringe a instalação do VDA.

A Citrix® agora assina todos os binários gerados pela Citrix com um certificado de assinatura de código da Citrix. Além disso, a Citrix também assina os binários de terceiros que são distribuídos com nosso produto com um certificado que autentica esses binários de terceiros como binários confiáveis.

> **Importante:**
>
> A atualização de um VDA mais antigo com binários de terceiros não assinados para uma versão mais recente do VDA com binários assinados pode nem sempre colocar os binários assinados na máquina atualizada. Isso se deve a um mecanismo dentro do sistema operacional onde a atualização do sistema não substitui binários com a mesma versão. Embora os binários de terceiros tenham sido assinados, suas versões, que são controladas por terceiros, não podem ser atualizadas pela Citrix, resultando na não atualização desses binários. Para evitar essa limitação:
>
> 1. Inclua os binários em uma lista de permissões. Isso elimina a necessidade de assinar os binários.
> 2. Desinstale o VDA mais antigo e instale o novo VDA. Isso se assemelha a uma instalação limpa do VDA e as versões assinadas serão instaladas.

### Criar uma nova Política Base com o Assistente

O WDAC permite adicionar binários confiáveis para serem executados em seu sistema. Após a instalação do WDAC, o **Assistente de Política de Controle de Aplicativos do Windows Defender** é aberto automaticamente.

Para adicionar os binários, uma nova política base do WDAC deve ser criada. As diretrizes recomendadas pela Citrix para criar uma política base são fornecidas nesta seção.

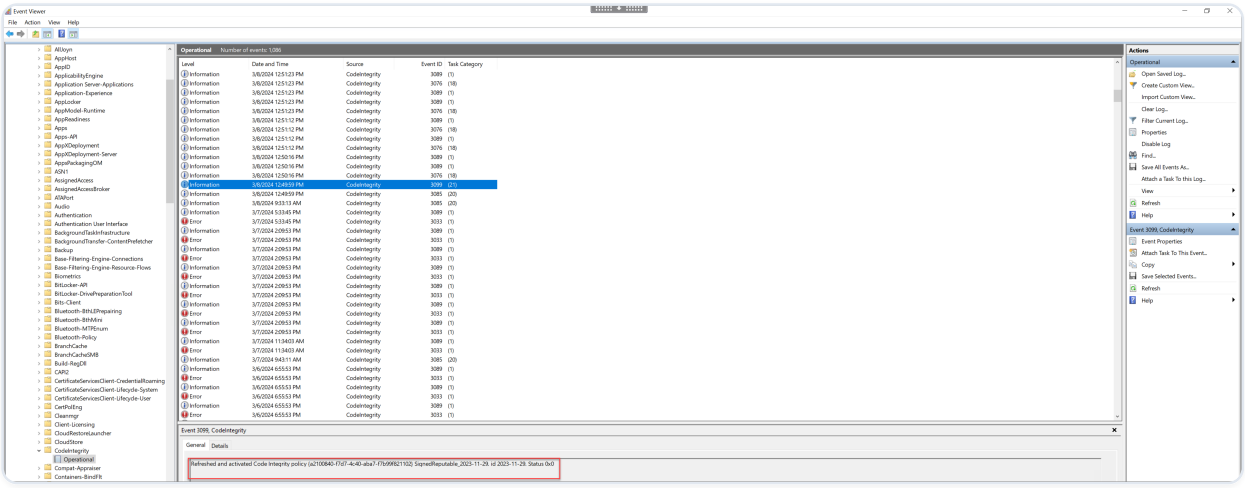
- Selecione o **Modo Assinado e Reputável** como modelo base porque ele autoriza componentes operacionais do Windows, aplicativos instalados da Microsoft Store, todo o software assinado pela Microsoft e drivers de hardware compatíveis com Windows de terceiros.
- **Habilite o Modo de Auditoria** porque ele permite testar novas políticas de Controle de Aplicativos do Windows Defender antes de aplicá-las.
- Adicione uma **Regra Personalizada** para **Regras de Arquivo** para especificar o nível no qual os aplicativos são identificados e confiáveis e forneça um arquivo de referência. Ao selecionar “Editor” como tipo de regra, um arquivo de referência assinado por um dos certificados Citrix pode ser selecionado.
- Depois que as regras forem adicionadas, navegar para a pasta onde os arquivos `.XML` e `.CIP` estão salvos. O arquivo `.XML` contém todas as regras definidas na política. Ele pode ser configurado para alterar, adicionar ou remover quaisquer regras.
- Antes de implantar as políticas do WDAC, o arquivo `.XML` deve ser convertido para sua forma binária. O arquivo WDAC converte o arquivo `.XML` para o arquivo `.CIP`.
- Copie e cole o arquivo `.CIP` em: C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active e reinicie a máquina. A política gerada será aplicada no modo de auditoria.
- Para um processo passo a passo para criar uma política base, consulte Criando uma nova Política Base com o Assistente.

Quando esta política é aplicada, o WDAC não emite avisos sobre quaisquer arquivos Citrix que sejam assinados pela autoridade de editor/CA especificada.

Da mesma forma, podemos criar uma regra de nível de editor para os arquivos que foram assinados por terceiros.

### Verificar a política aplicada

1. Após a reinicialização da máquina, abra o **Visualizador de Eventos** e vá para **Logs de Aplicativos e Serviços > Microsoft > Windows > CodeIntegrity > Operacional**.
2. Certifique-se de que a política aplicada esteja ativada.



3. Procure por logs que violaram a política e verifique as propriedades desse arquivo. Primeiro, confirme se ele foi assinado. Se não foi e esta máquina passou por uma atualização de VDA, este é provavelmente o caso descrito na limitação acima. Se assinado, este arquivo está potencialmente assinado com o certificado alternativo, conforme descrito anteriormente.

Um exemplo de arquivo gerado pela Citrix assinado com um certificado Citrix é `C:\Windows\System32\drivers\picadm.sys`. Um exemplo de binário de terceiros assinado com o certificado de terceiros da Citrix é `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

# Instalar VDAs usando SCCM

## Visão geral

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

> **Nota:**
>
> O artigo a seguir descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

### Recomendações

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

### Antes de começar

O número de reinicializações necessárias durante a instalação do VDA depende do ambiente. Por exemplo:

- Uma reinicialização pode ser necessária para atualizações pendentes ou reinicializações de instalações de software anteriores.
- Arquivos previamente bloqueados por outros processos podem precisar de atualizações, forçando uma reinicialização extra.
- Alguns componentes opcionais no instalador do VDA (como Citrix Profile Management e Citrix Files) podem exigir uma reinicialização.
- Ao atualizar um VDA, a máquina na qual ele está instalado deve estar no modo de manutenção, sem sessões.
- Quando uma instalação do VDA é executada pela primeira vez em uma máquina, o instalador do VDA que está sendo usado é copiado para essa máquina. Para obter mais informações sobre a instalação do VDA, consulte Instaladores.

**O Sequenciador de Tarefas do SCCM** gerencia todas as reinicializações necessárias.

### Etapas principais para implantar o VDA usando SCCM

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

1. Instalar o VDA.
2. Criar uma unidade organizacional (OU).
3. Verificar as máquinas.
4. Usar VDA para distribuir conteúdo.

### Etapa 1: Instalar o VDA

Depois de identificar todos os pré-requisitos, use o **SCCM Task Sequencer** para concluir as seguintes tarefas:

1. Instale o VDA a partir de uma cópia acessível da mídia de instalação ou de um dos instaladores autônomos do VDA:

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   Para obter mais informações sobre os instaladores do VDA, consulte Instaladores.

   > **Nota:**
   >
   > Ao atualizar um VDA, a máquina na qual ele está instalado deve estar em modo de manutenção, sem sessões.

2. Quando uma instalação do VDA é executada pela primeira vez em uma máquina, o instalador do VDA que está sendo usado é copiado para essa máquina.

   - Quando você usa um instalador VDA diferente de `VDAWorkstationCoreSetup_XXXX.exe`, o instalador VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
   - Quando você usa `VDAWorkstationCoreSetup_XXXX.exe`, o instalador VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`.

3. O local do diretório do instalador do VDA também é armazenado no registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”`.

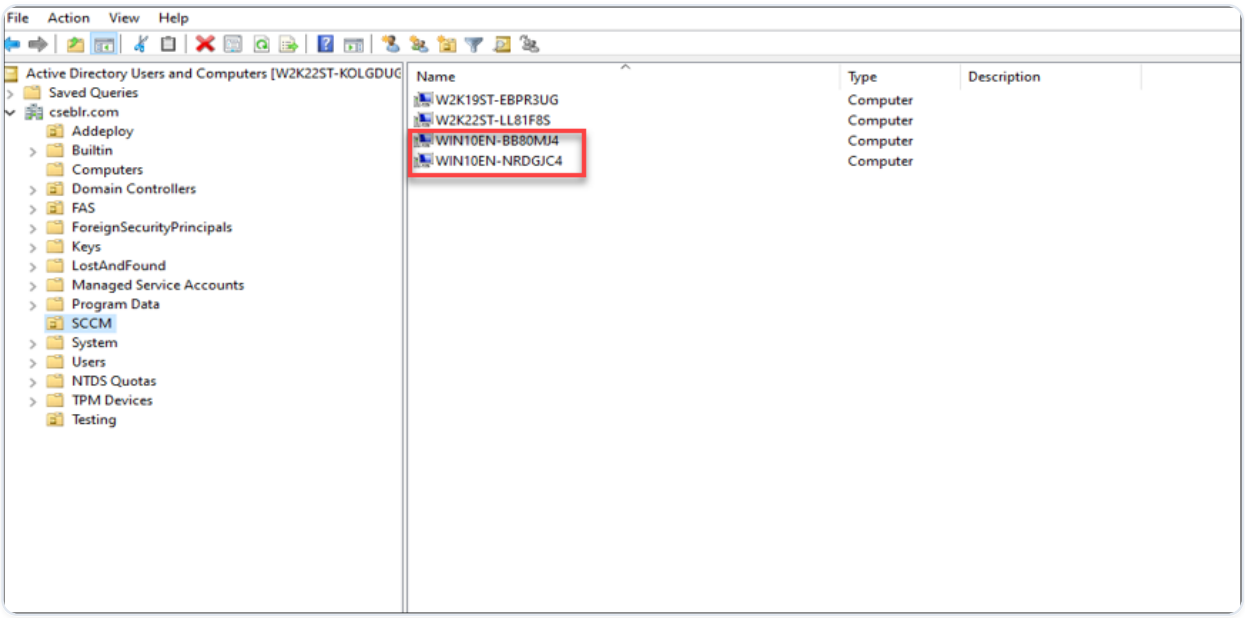
4. Adicione as opções de linha de comando `/NOREBOOT`, `/NORESUME` e `/QUIET` às suas opções de linha de comando.

   - `/QUIET`: Não mostre a interface do usuário durante a instalação, para que o SCCM tenha controle do processo de instalação.
   - `/NOREBOOT`: Suprima a reinicialização automática do instalador do VDA. O SCCM aciona as reinicializações quando necessário.

- `/NORESUME`: Geralmente, quando uma reinicialização é necessária 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 reinicia. Isso é um problema para o SCCM, porque o SCCM não consegue monitorar a instalação e capturar o código de saída.

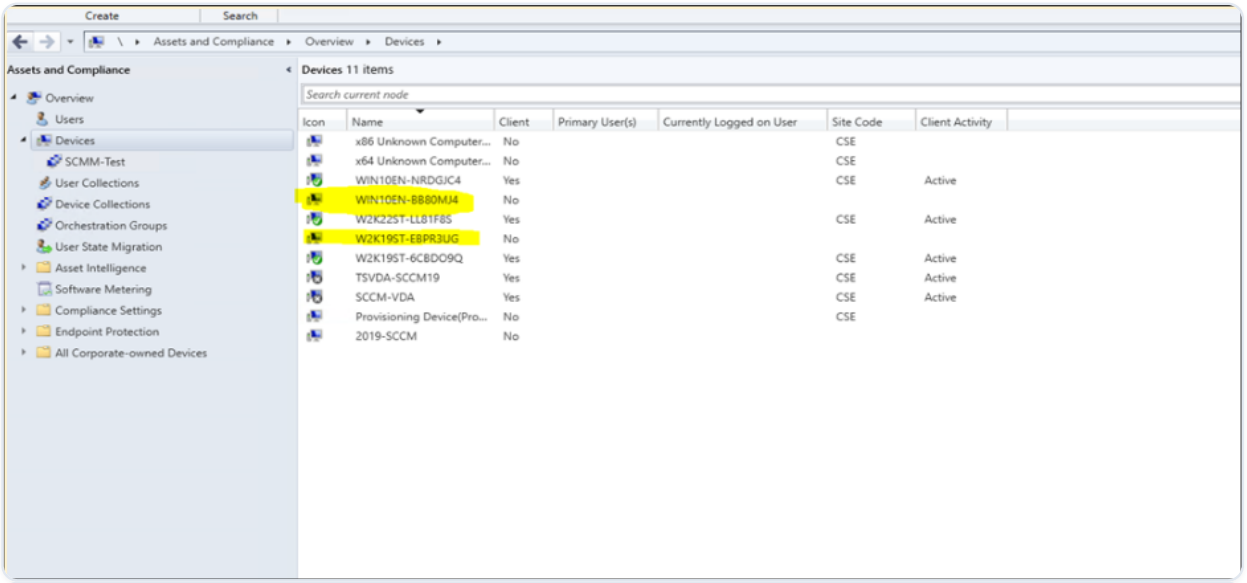
### Etapa 2: Criar uma unidade organizacional (OU)

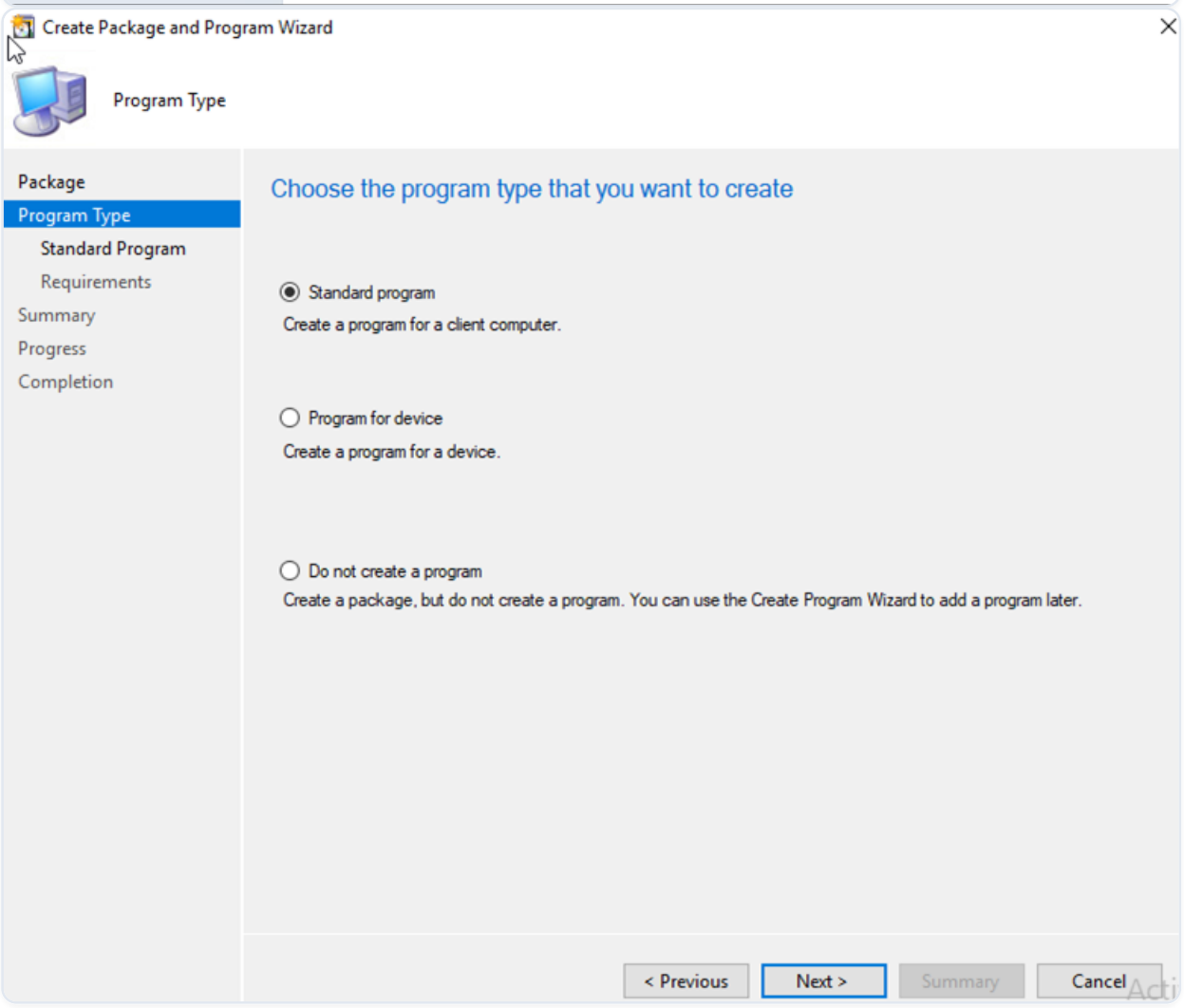
1. Crie duas máquinas virtuais ingressadas no domínio que você deseja adicionar à OU. Quando as máquinas virtuais são criadas inicialmente, elas estão na pasta **Computers**. Mova as máquinas virtuais para a pasta **SCCM**. Exemplo: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com



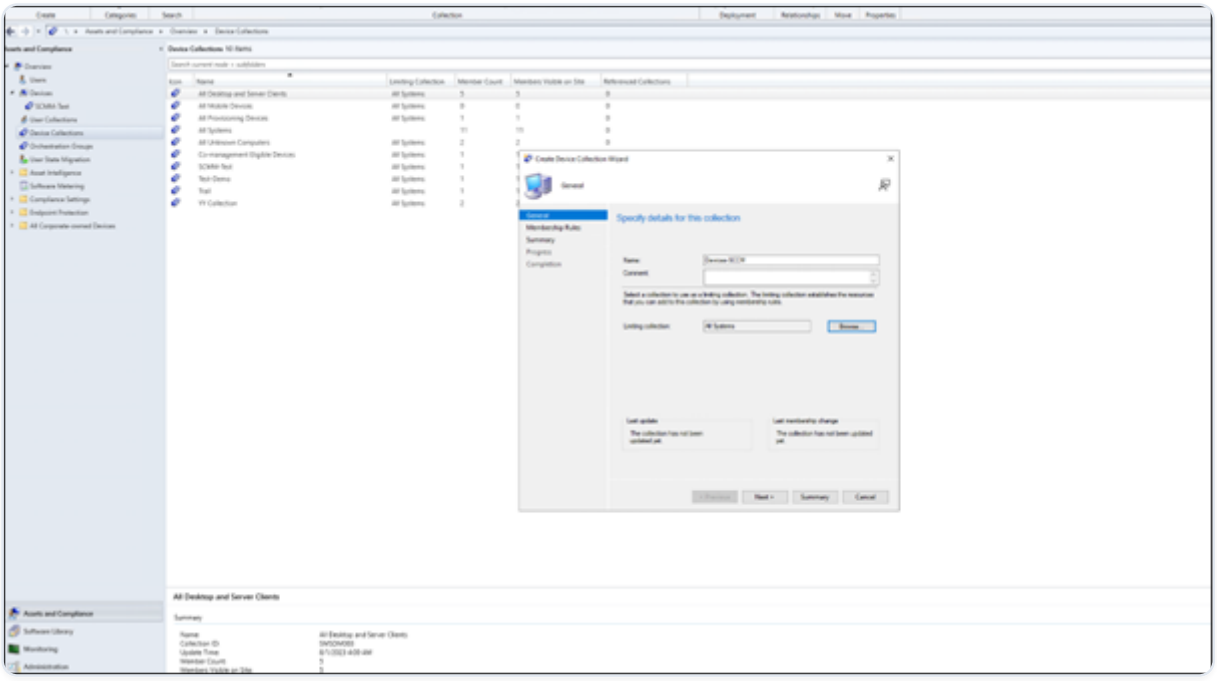

2. No Microsoft Configuration Manager, vá para `\Administration\Overview\Hierarchy Configuration\Discovery Methods\`.
3. Clique em **Active Directory System Discovery** e selecione a caixa de seleção **Enable Active Directory System Discovery** para habilitar a descoberta automática das máquinas virtuais recém-criadas.
4. Clique no ícone  para selecionar novos contêineres.
5. Na seção **Location**, adicione o **Path** onde suas máquinas virtuais SCCM estão localizadas.
6. Vá para `\Administration\Overview\Site Configuration\Sites` e clique com o botão direito do mouse no SCCM VDA.
7. Selecione **Client Installation Settings > Client Push Installation**. A janela **Client Push Installation Properties** é aberta.

8. Depois que as VMs forem definidas como `Enabled`, você poderá ver a lista de VMs, conforme ilustrado nas imagens a seguir.

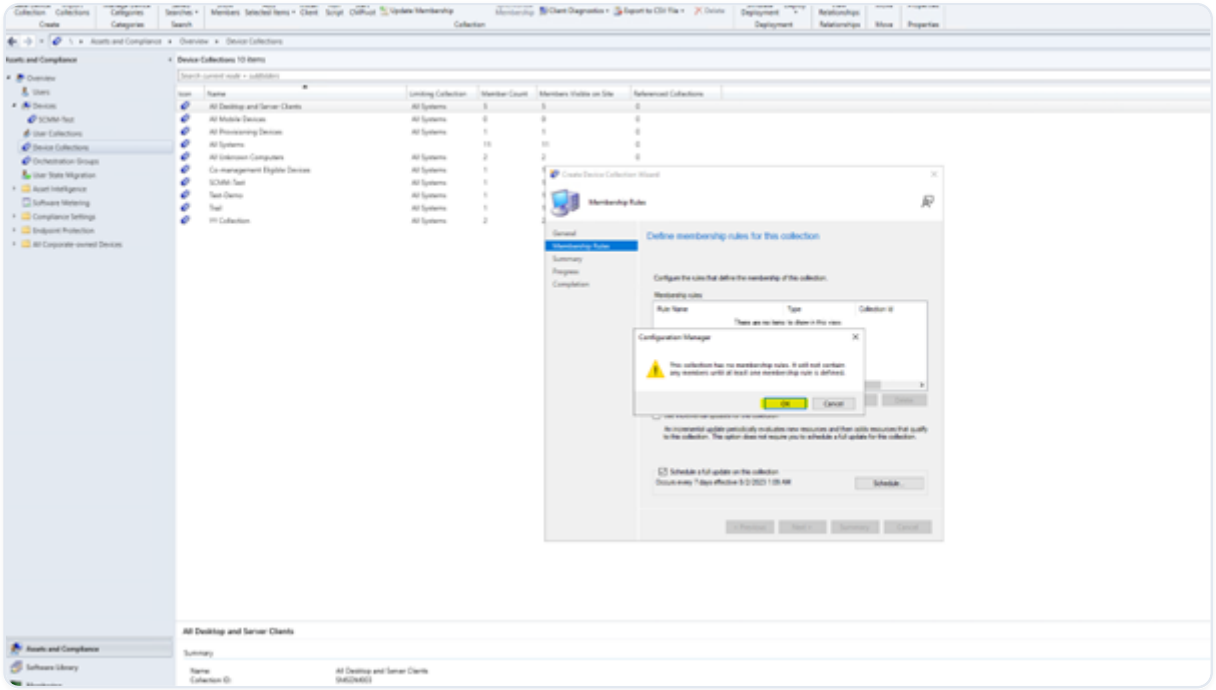


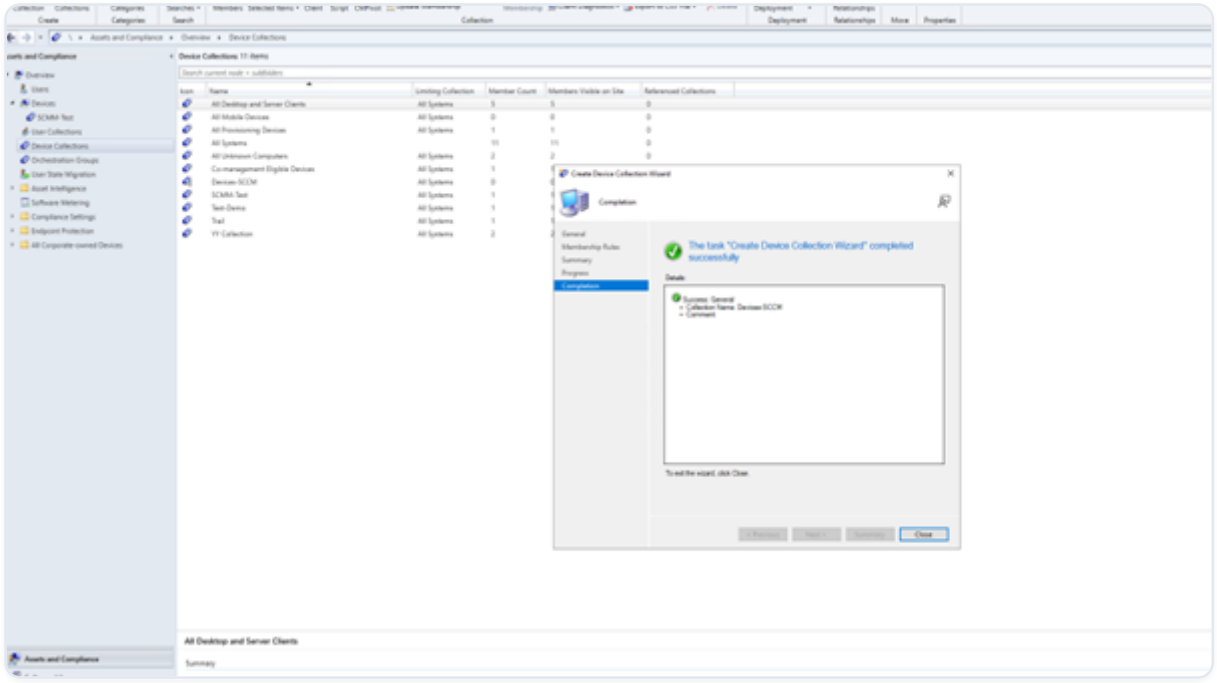

9. Crie a **Device collection** para criar a OU. Insira o **Name** do Nome da Coleção.



10. Siga as instruções do assistente.

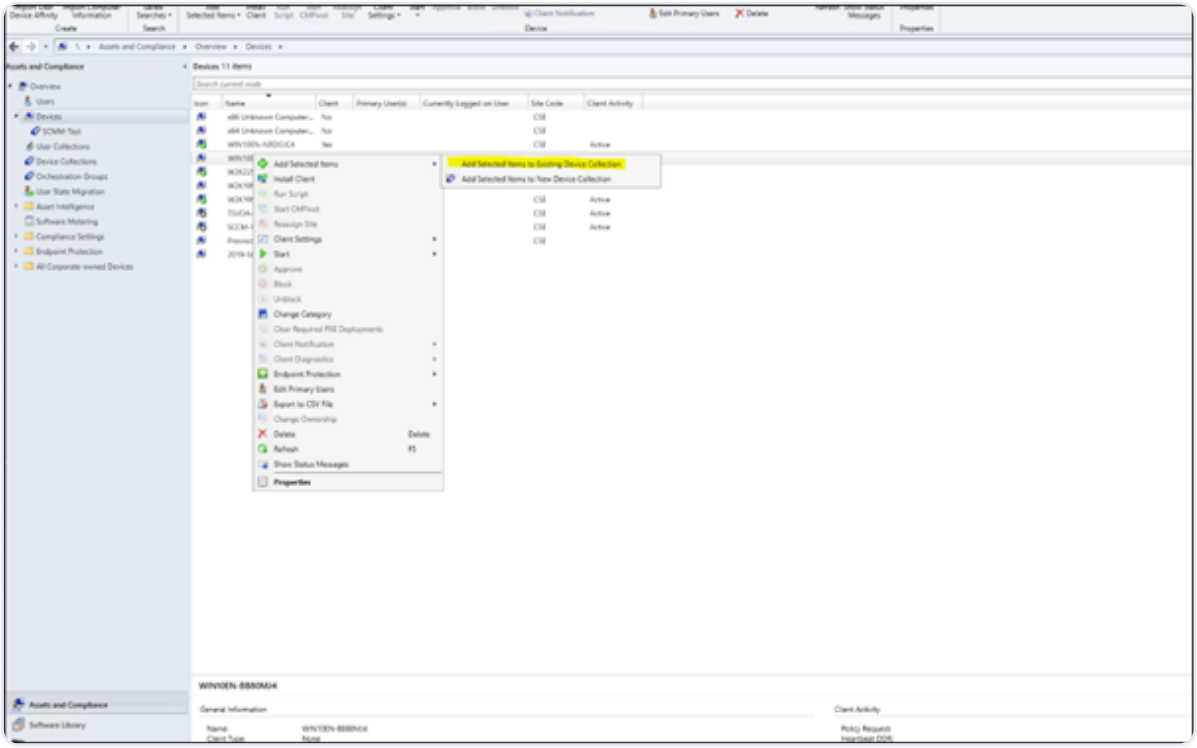


A OU é criada.

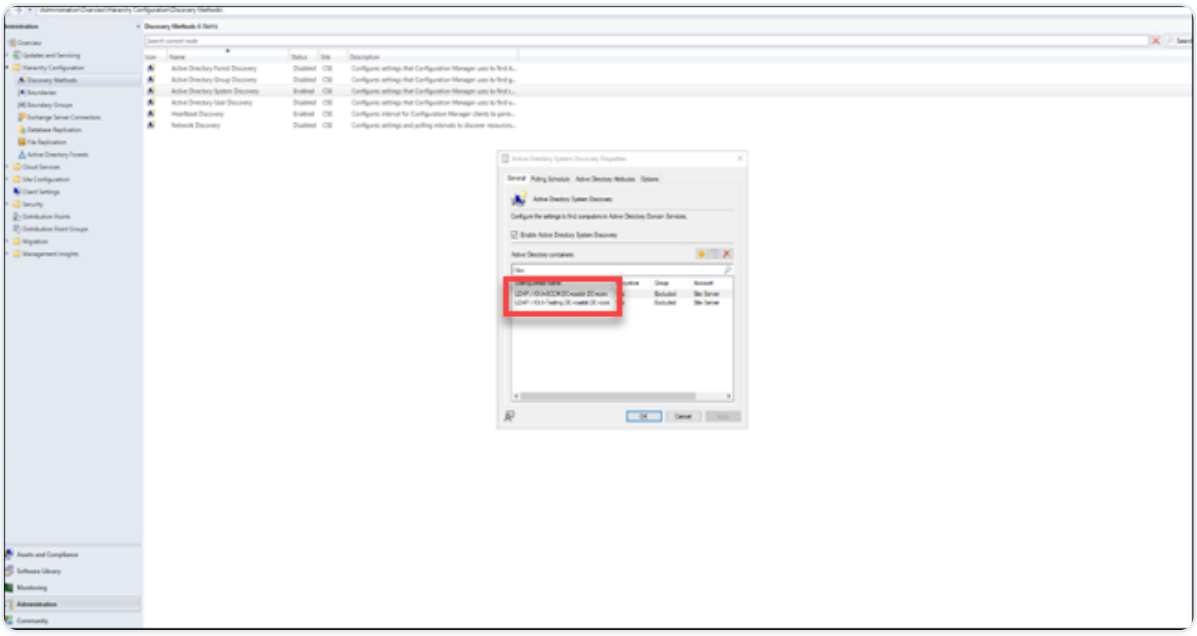


11. Adicione as VMs criadas à Coleção de Dispositivos recém-criada.

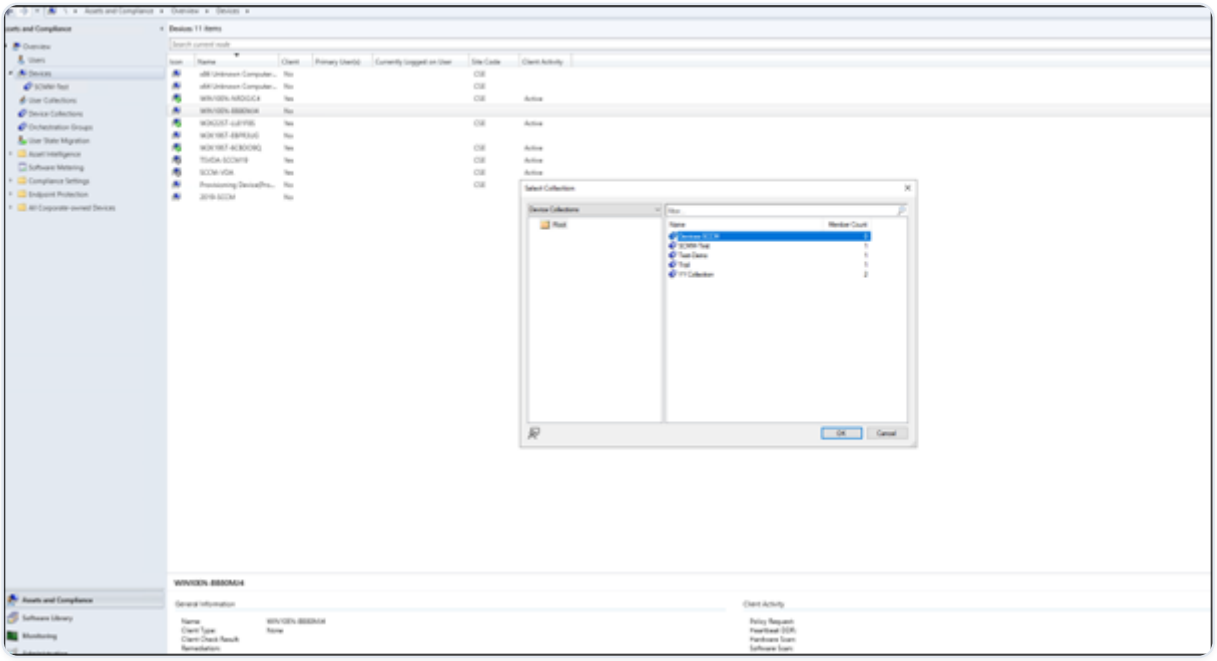
    a. Clique com o botão direito na VM. Selecione **Adicionar Itens Selecionados > Adicionar Itens Selecionados à Coleção de Dispositivos Existente**.



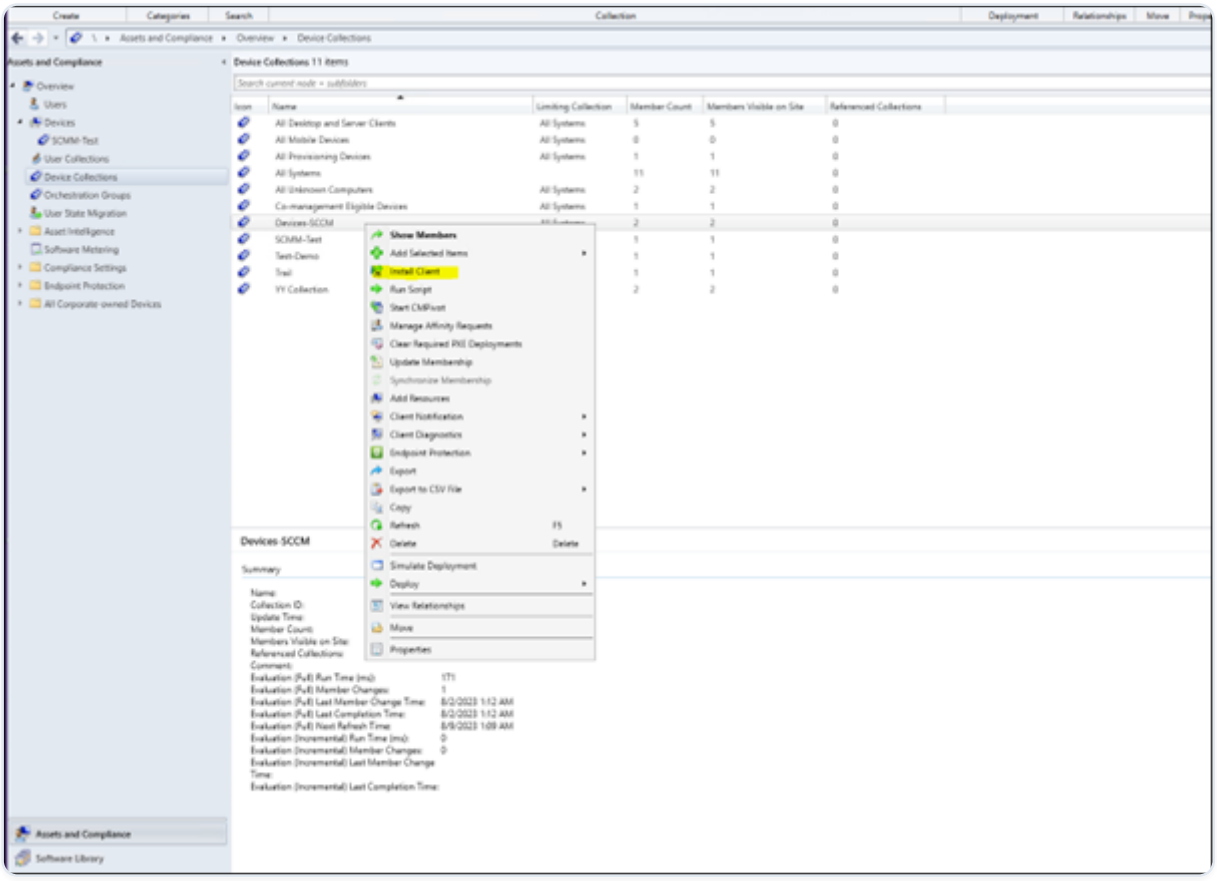
    b. Na janela **Selecionar Coleção**, selecione o nome do dispositivo necessário. Neste exemplo, é `Devices-SCCM`.



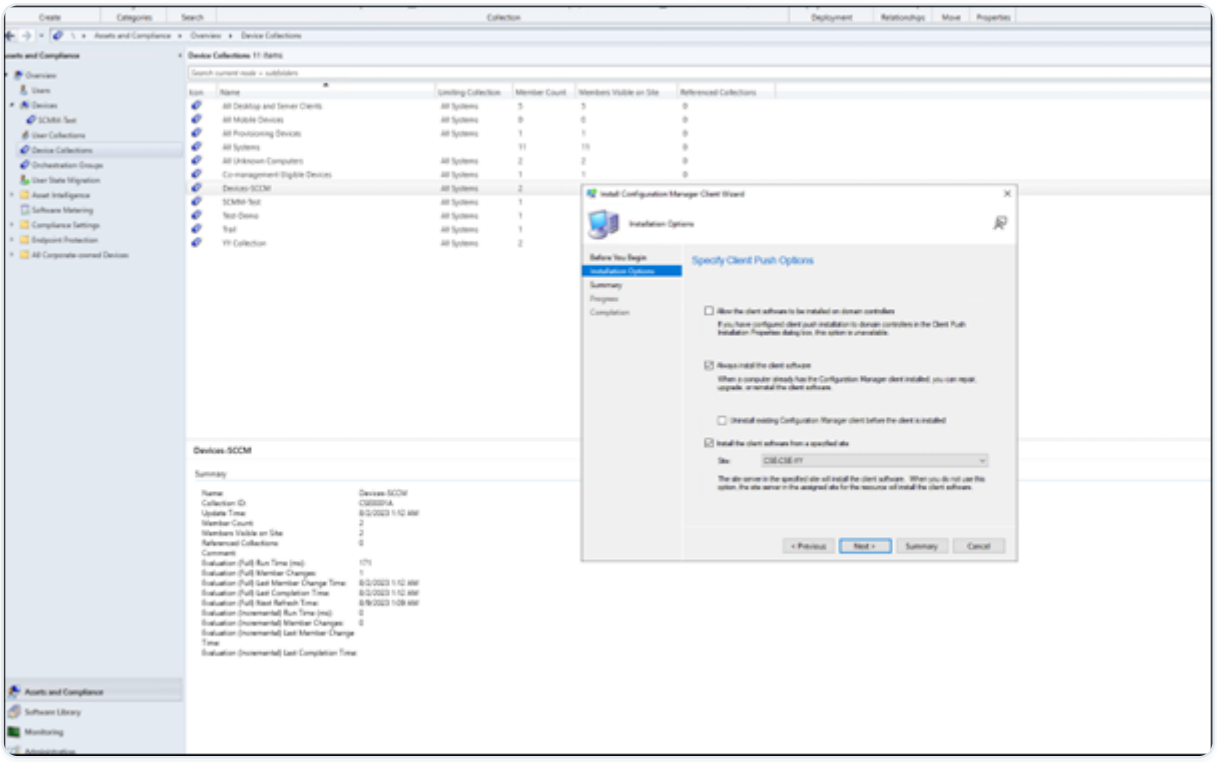
`Devices-SCCM` está listado em **Ativos e Conformidade > Visão Geral > Coleções de Dispositivos**.



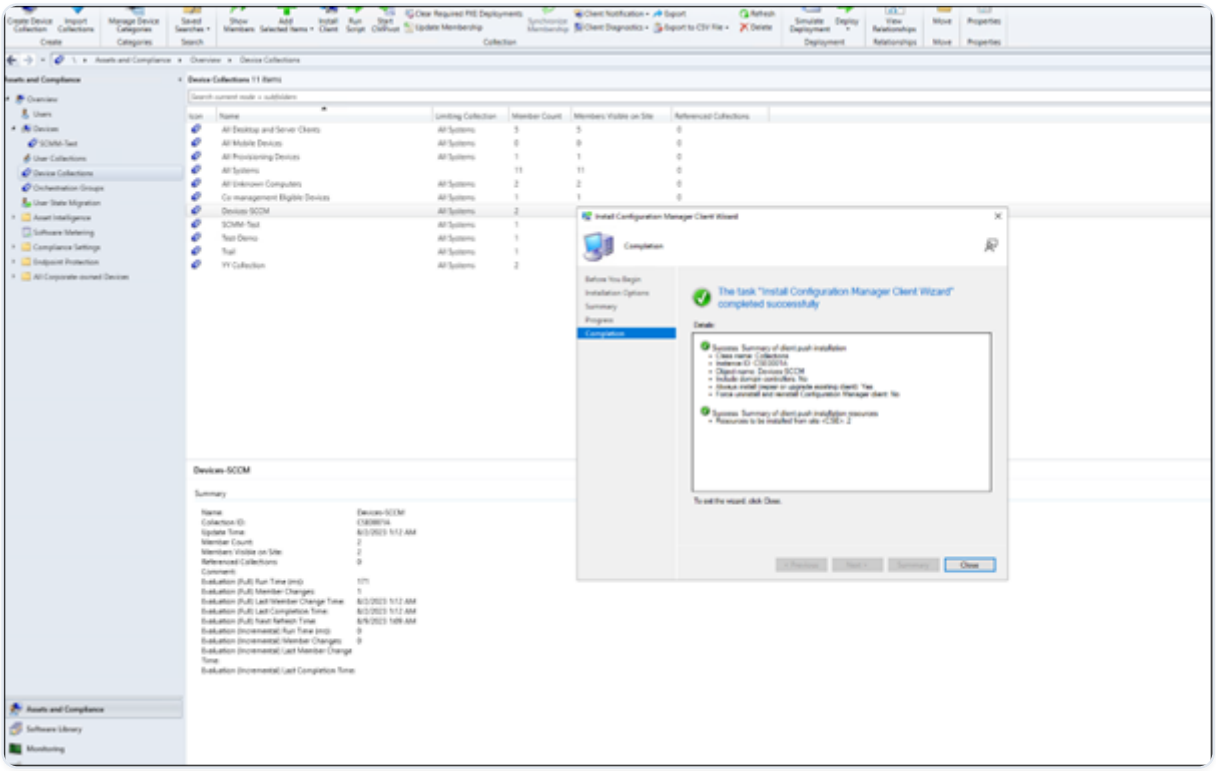
12. Selecione **Instalar Cliente** no Coletor de Dispositivos.



13. Selecione o **Site** de instalação necessário.



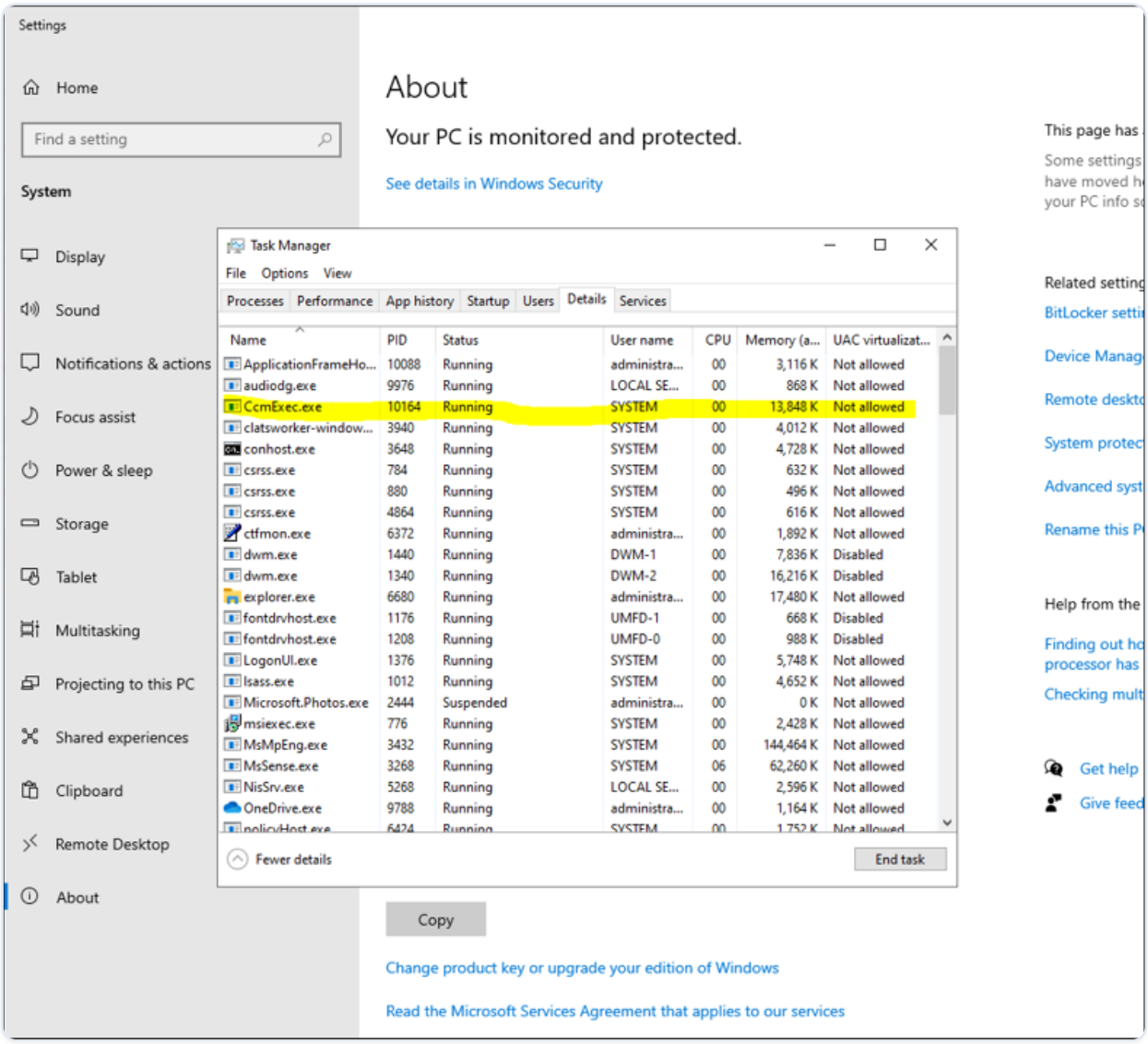
14. Siga as instruções do assistente. O **Assistente de Instalação do Cliente do Configuration Manager** foi concluído com êxito.



Para obter informações detalhadas, consulte Gerenciar coleções na documentação da Microsoft.

### Etapa 3: Verificar as máquinas

1. Na máquina cliente, verifique se o cliente está instalado, verificando se o processo `CCMExec` está em execução.




2. Verifique se o Cliente está em execução para as VMs no SCCM.

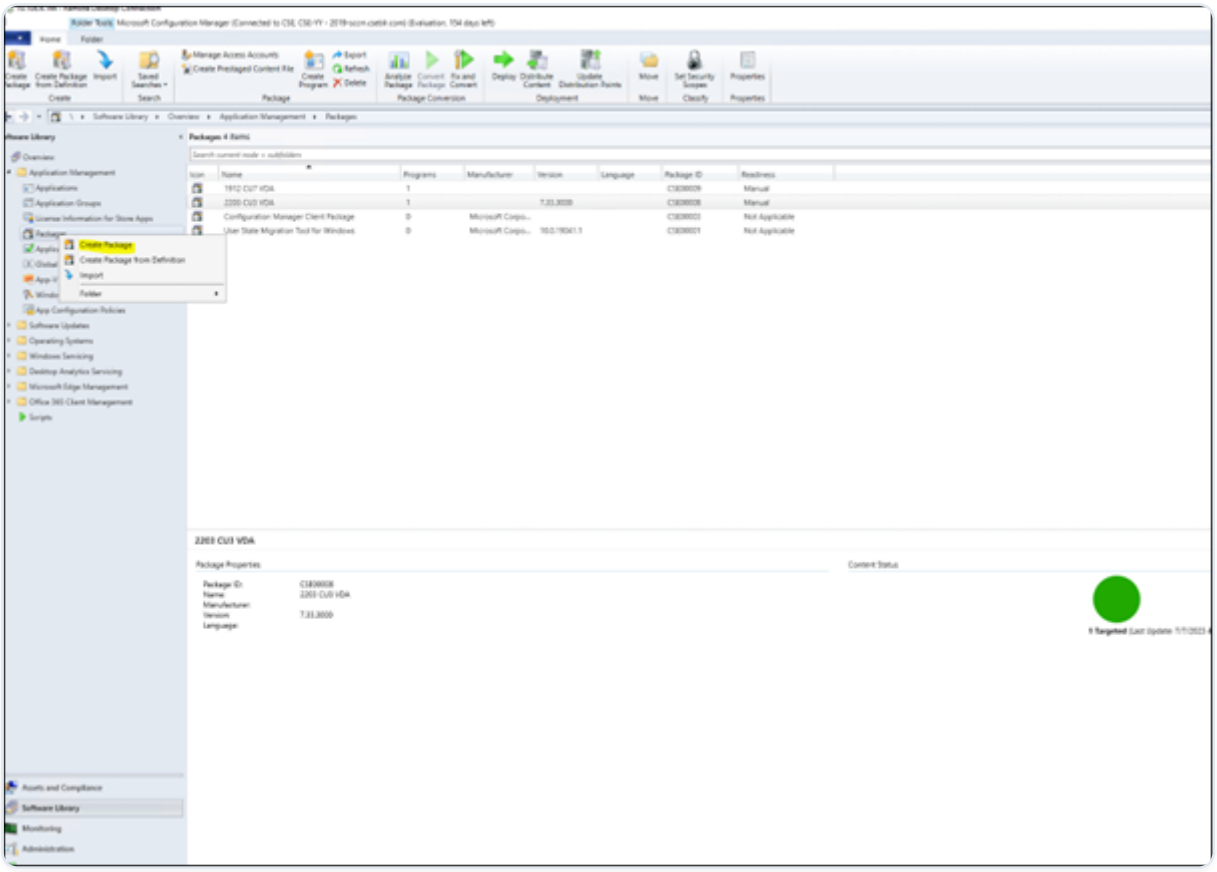
### Passo 4: Usar VDA para distribuir conteúdo

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

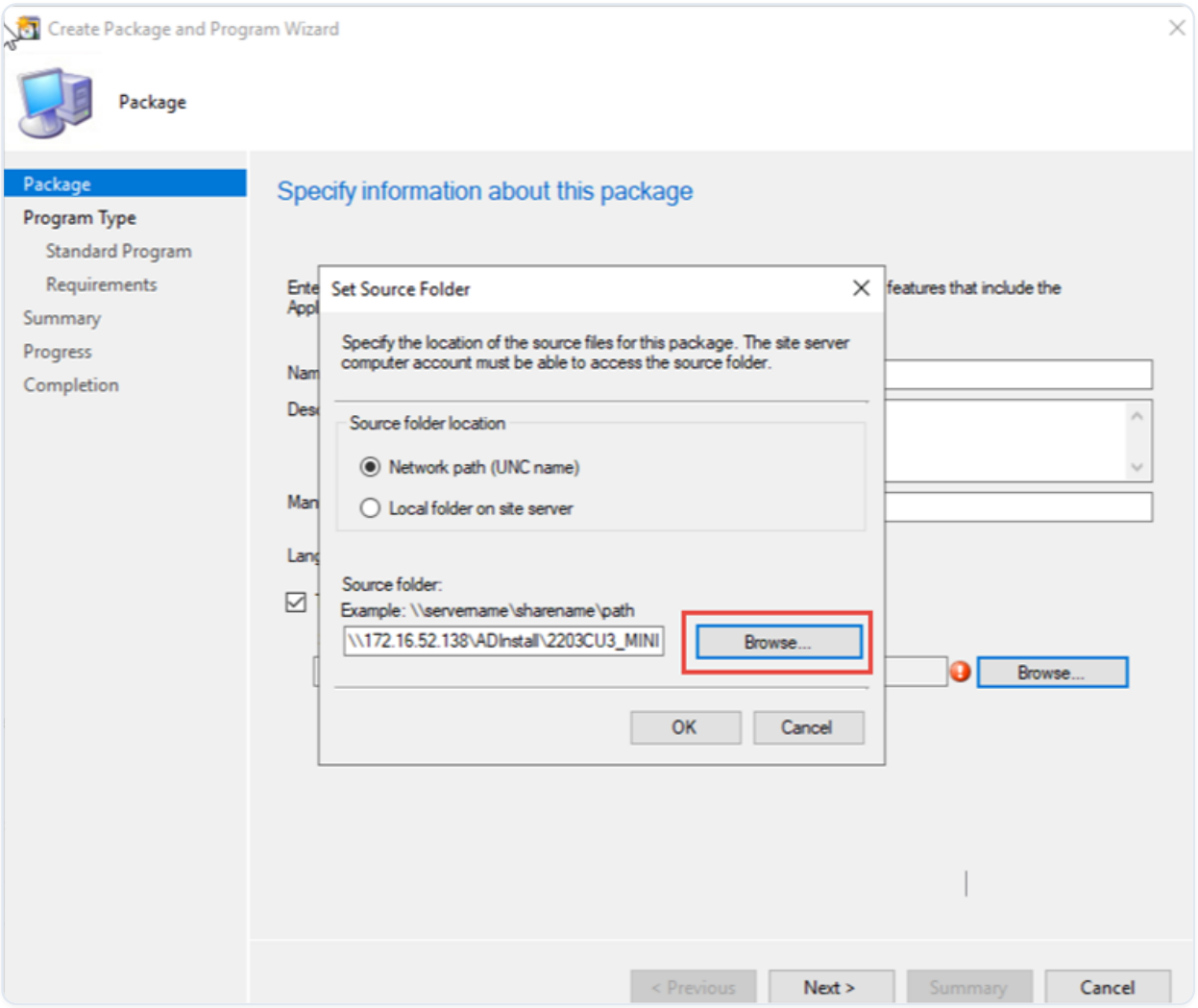
1. Criar um pacote
2. Distribuir conteúdo

#### CRIAR UM PACOTE

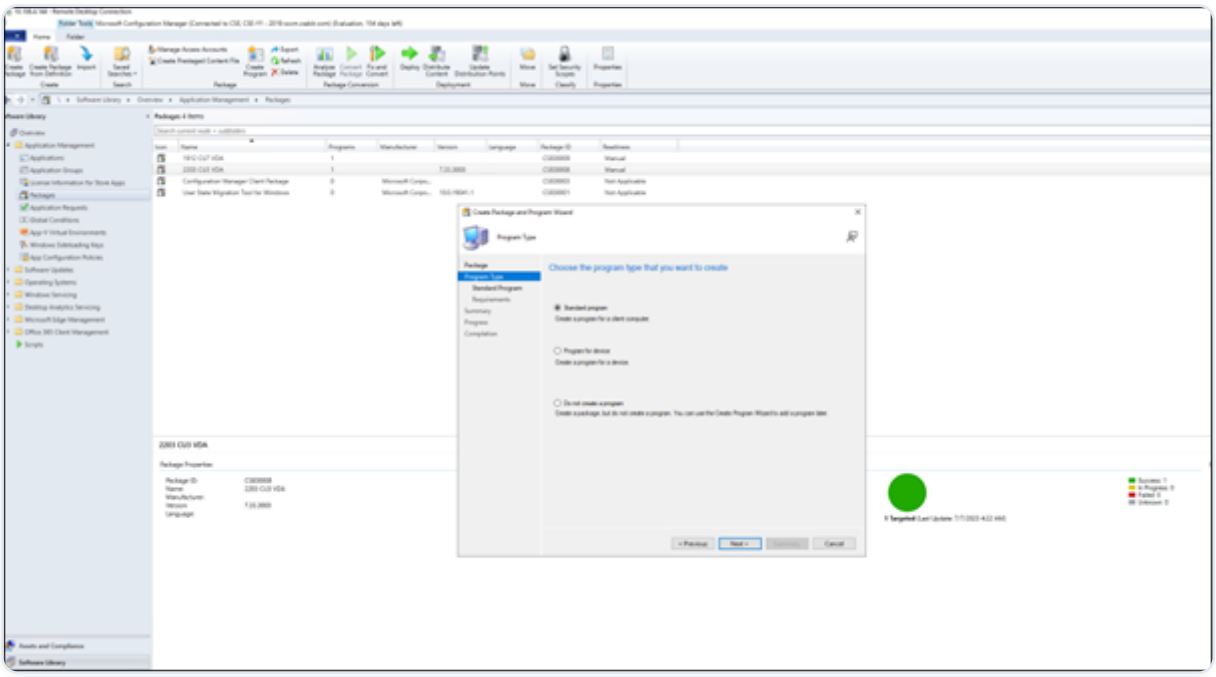
1. Para criar um pacote, clique com o botão direito do mouse no VDA desejado e clique em **Criar Pacote**.



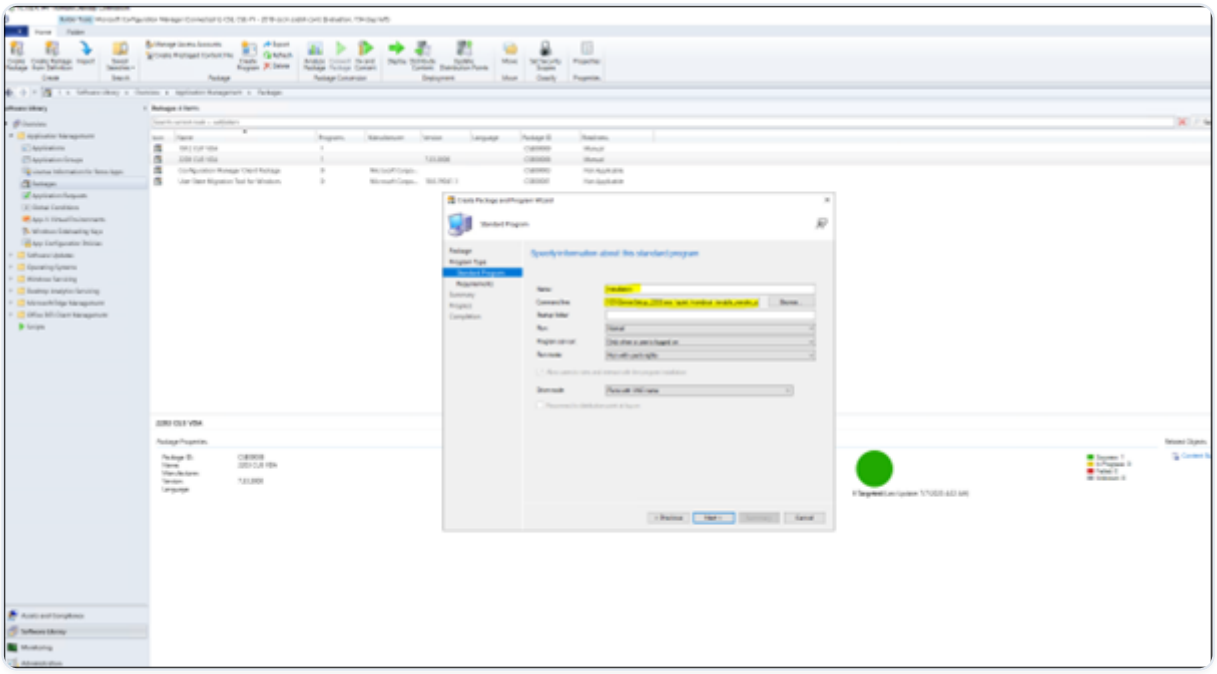
2. Especifique o local dos arquivos de origem para este pacote clicando em **Procurar**.



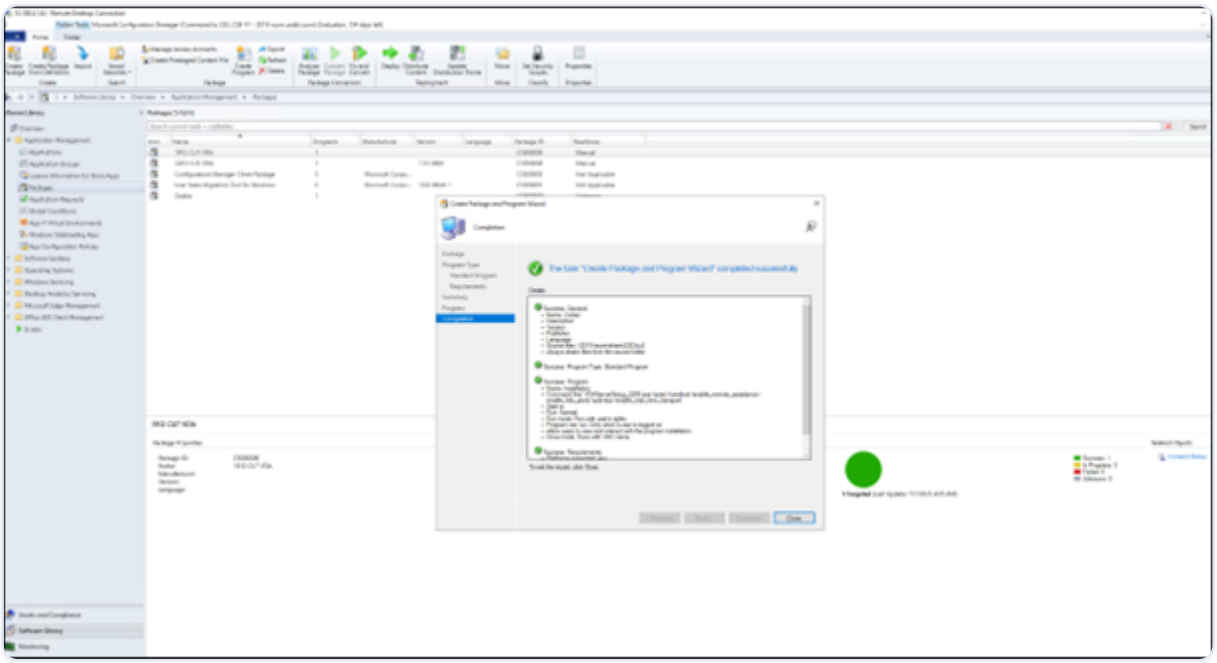

3. Selecione o tipo de pacote desejado.



4. Insira o **Nome** do pacote e a **Linha de comando**.



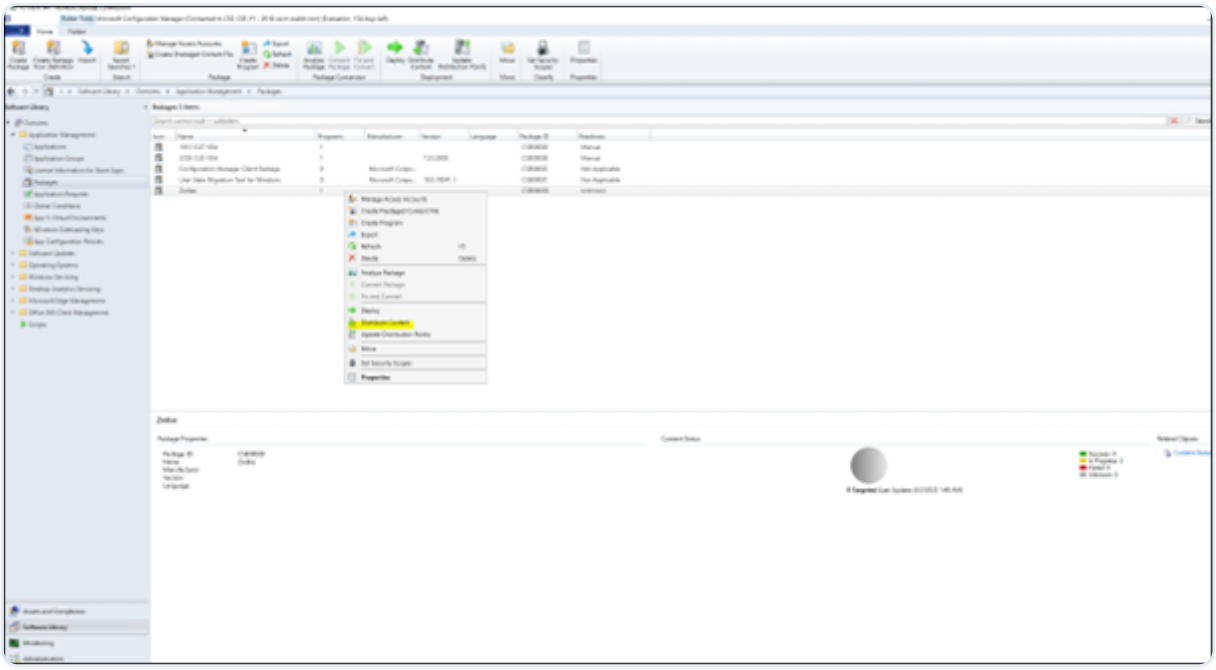
5. Clique em **Avançar**.



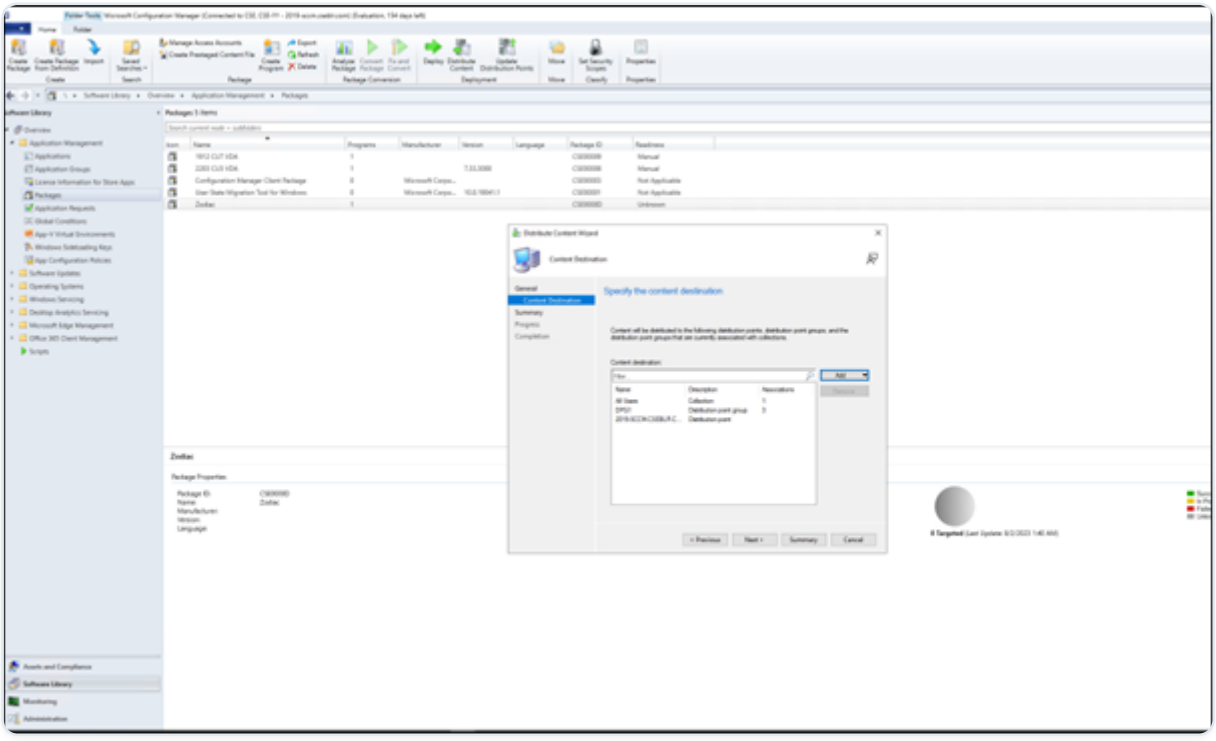
Para obter informações detalhadas, consulte Pacotes e programas no Configuration Manager na documentação da Microsoft.

### DISTRIBUIR CONTEÚDO

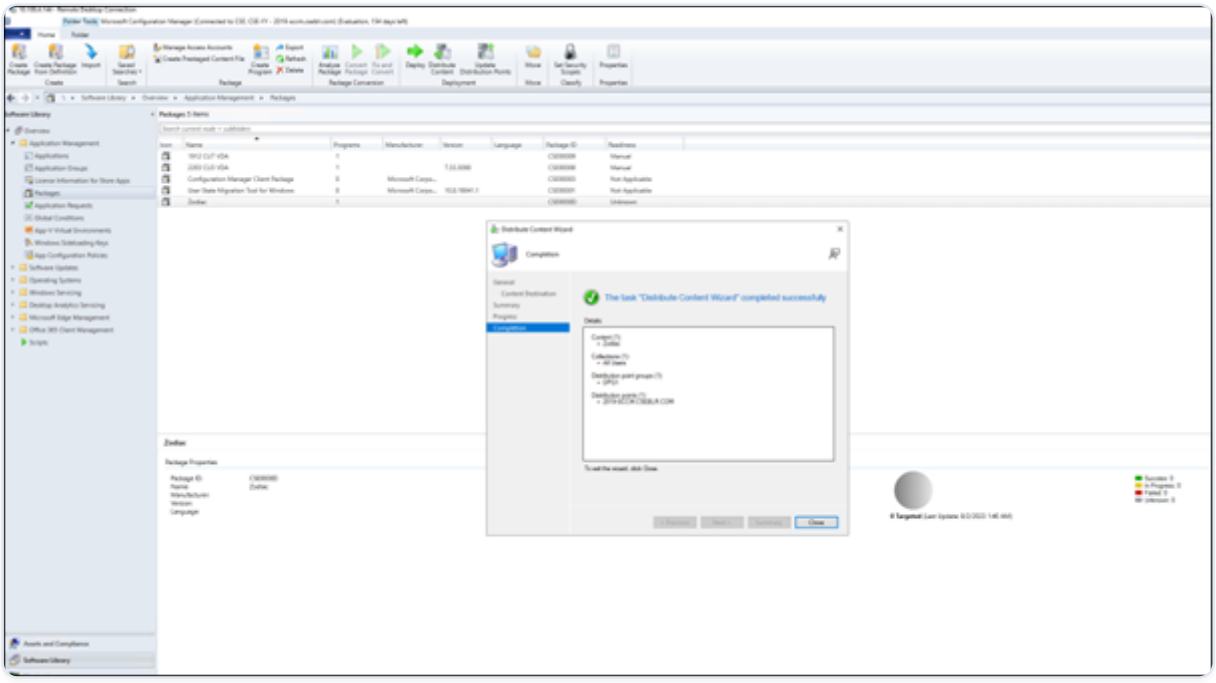
1. Clique com o botão direito do mouse no nome do pacote que você criou.
2. Selecione **Distribuir Conteúdo**.



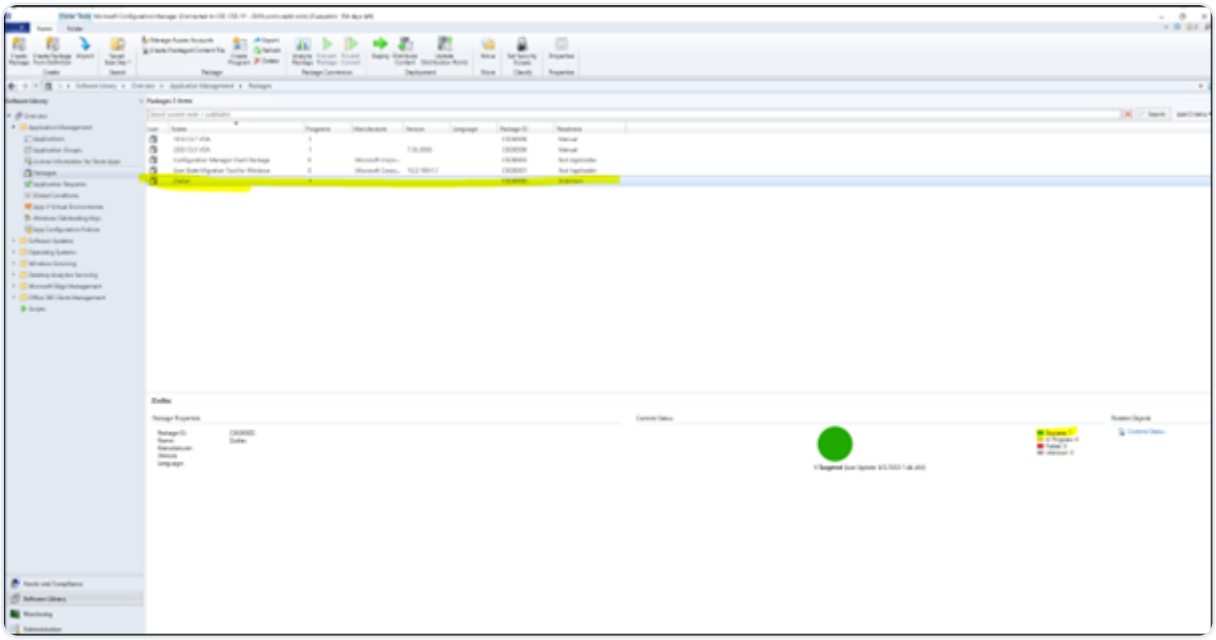
3. Na janela do **Assistente para Distribuir Conteúdo**, selecione o local dos arquivos de origem para o pacote que você criou. Neste exemplo, é `2019-SCCM`. Clique em **Avançar**.



4. Verifique se o Pacote (neste exemplo, `Zodiac`) está disponível para implantação.



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

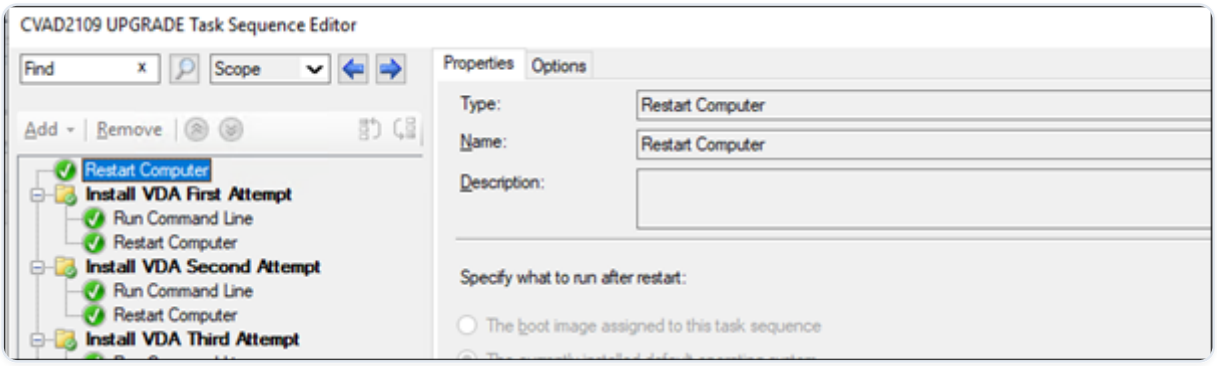


Para obter informações detalhadas, consulte Implantar e gerenciar conteúdo para Configuration Manager na documentação da Microsoft.

### Exemplo de sequência de instalação usando SCCM

O exemplo a seguir mostra a sequência de instalação.

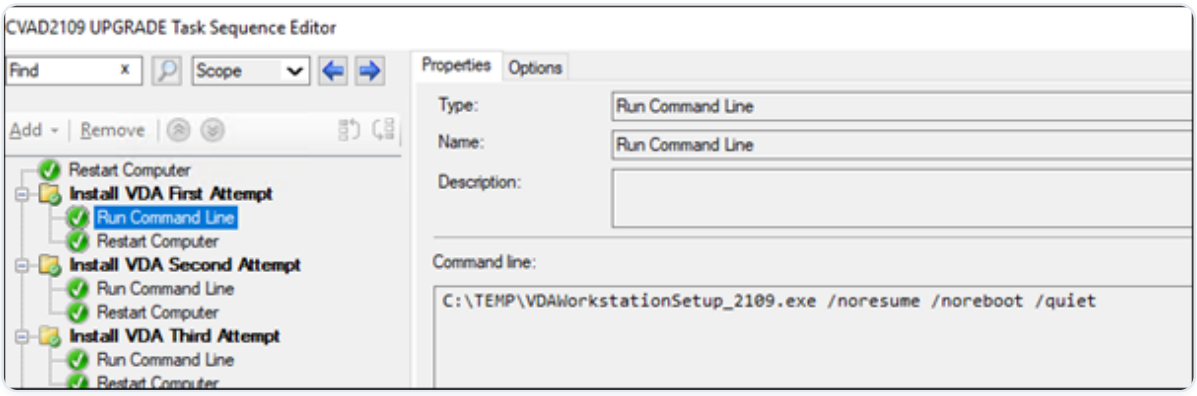
1. **Reiniciar computador:** Prepare a máquina reiniciando-a.




2. **Instalar VDA Primeira Tentativa:** Inicie a instalação do VDA.

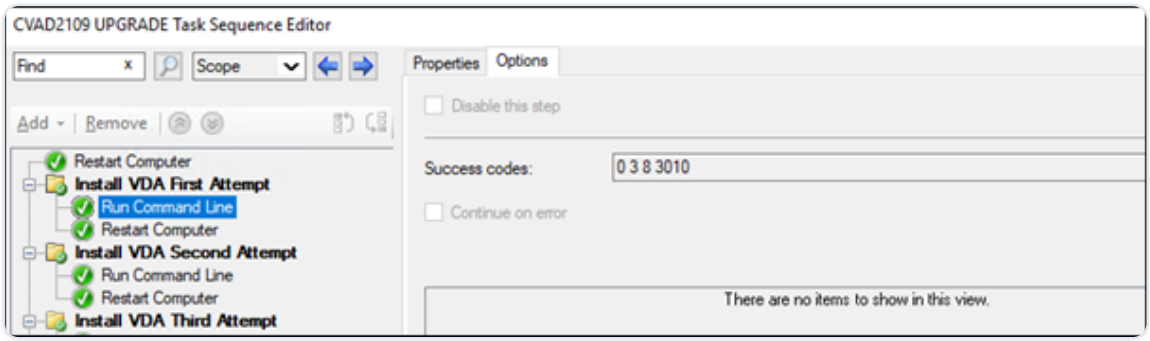
   a. Adicione as opções `/quiet`, `/noreboot` e `/noresume` às suas opções de linha de comando.

   b. Execute o instalador do VDA de sua escolha (imagem local ou um dos instaladores mínimos).

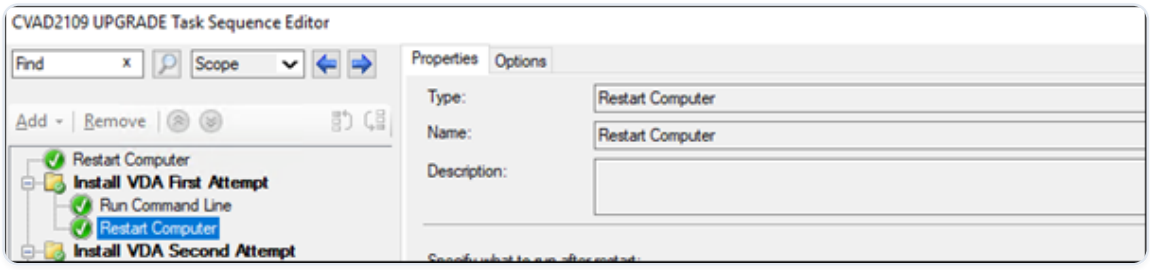



   c. O SCCM deve capturar o código de retorno.

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




      - Se o código de retorno for 3, reinicie a máquina e, em seguida, passe o controle para **Instalar VDA Segunda Tentativa**.



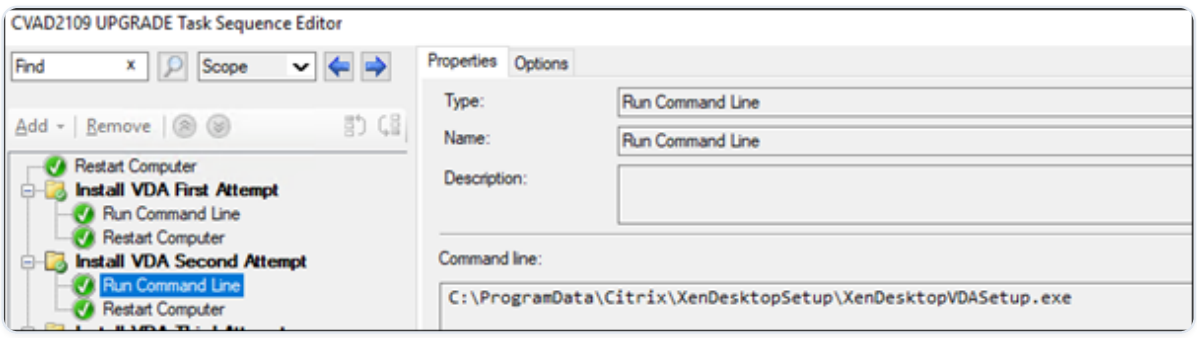

3. **Segunda Tentativa de Instalação do VDA:** Continuar a instalação do VDA.

   a. Após a **Primeira Tentativa de Instalação do VDA** se o arquivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` existir, a instalação não está completa e deve ser continuada após a conclusão da reinicialização.



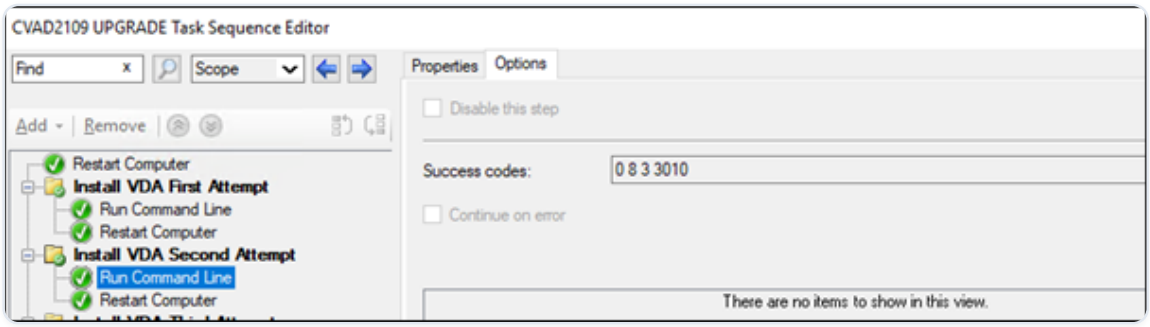

   b. **Segunda Tentativa de Instalação do VDA** se repete até que o arquivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` não exista ou um código de retorno diferente de 0 ou 8 seja retornado. Trate qualquer outro código de retorno como um erro, e a SEGUNDA TENTATIVA DE INSTALAÇÃO DO VDA deve relatar um erro e parar.

   c. Retome a instalação do VDA executando o instalador VDA apropriado (`XenDesktopVdaSetup.exe` para a maioria dos casos, ou `XenDesktopRemotePCSetup.exe` se `VDAWorkstationCoreSetup_XXXX.exe` foi usado) do diretório do arquivo `%programdata%\ Citrix\XenDesktopSetup\` sem parâmetros de linha de comando. (O instalador VDA usa os parâmetros que salvou durante a primeira execução do instalador.)



d. Observe o código de retorno do instalador VDA.

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




- 3: A instalação não está completa. Reinicie a máquina e repita a SEGUNDA TENTATIVA DE INSTALAÇÃO DO VDA 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 a SEGUNDA TENTATIVA DE INSTALAÇÃO DO VDA deve relatar um erro e terminar.

Para obter mais informações sobre códigos de retorno, consulte códigos de retorno de instalação do Citrix.

### Exemplos de comando de instalação do VDA

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

- Instalar VDAs
- Instalar usando a linha de comando

#### Comandos de instalação para Acesso Remoto ao PC

- O seguinte comando usa o instalador VDA principal de sessão única (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- O seguinte comando usa o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

### Comando de instalação para VDI dedicado

- O comando a seguir usa o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers "control.domain.com" /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

## Instalar VDAs usando scripts

> **Nota:**

> A Citrix não se responsabiliza por problemas causados por scripts adaptados para corresponder aos ambientes de produção do cliente. Para quaisquer problemas da Citrix relacionados à instalação, abra um caso de suporte técnico com os logs de instalação relevantes usando o portal de Suporte da Citrix.

> Este artigo se aplica à instalação de VDAs em máquinas com sistemas operacionais Windows. Para obter informações sobre VDAs para sistemas operacionais Linux, consulte a documentação do Linux Virtual Delivery Agent.

A mídia de instalação contém scripts de exemplo que instalam, atualizam ou removem Virtual Delivery Agents (VDAs) para máquinas no Active Directory. Você também pode usar os scripts para manter imagens mestre usadas pelo Machine Creation Services™ e Citrix Provisioning (anteriormente Provisioning Services).

Acesso necessário:

- Os scripts precisam de acesso de Leitura para Todos (Everyone Read) ao compartilhamento de rede onde o comando de instalação do VDA está localizado. O comando de instalação é `XenDesktopVdaSetup.exe` no ISO completo do produto, ou `VDAWorkstationSetup.exe` ou `VDAServerSetup.exe` em um instalador autônomo.
- Os detalhes de log são armazenados em cada máquina local. Para registrar os resultados centralmente para revisão e análise, os scripts precisam de acesso de Leitura e Gravação para Todos (Everyone Read and Write) ao compartilhamento de rede apropriado.

Para verificar os resultados da execução de um script, examine o compartilhamento de log central. Os logs capturados incluem o log do script, o log do instalador e os logs de instalação do MSI. Cada tentativa de instalação ou remoção é registrada em uma pasta com carimbo de data/hora. O título da pasta indica o resultado da operação com o prefixo PASS ou FAIL. Você pode usar ferramentas de pesquisa de diretório padrão para encontrar uma instalação ou remoção com falha no compartilhamento de log central. Essas ferramentas oferecem uma alternativa à pesquisa local nas máquinas de destino.

Antes de iniciar qualquer instalação, leia e conclua as tarefas em Preparar para instalar.

### Instalar ou atualizar VDAs usando o script

1. Obtenha o script de exemplo **InstallVDA.bat** de `\Support\AdDeploy\` na mídia de instalação. A Citrix recomenda que você faça um backup do script original antes de personalizá-lo.
2. Edite o script:
   - Especifique a versão do VDA a ser instalada: `SET DESIREDVERSION`. O valor completo pode ser encontrado na mídia de instalação no arquivo ProductVersion.txt. No entanto, uma correspondência completa não é necessária.
   - Especifique o compartilhamento de rede onde o instalador será invocado. Aponte para a raiz do layout (o ponto mais alto da árvore). A versão apropriada do instalador (32 bits ou 64 bits) é chamada automaticamente quando o script é executado. Por exemplo: `SET DEPLOYSHARE=\\fileserver1\share1`.
   - Opcionalmente, especifique um local de compartilhamento de rede para armazenar logs centralizados. Por exemplo: `SET LOGSHARE=\\fileserver1\log1)`.
   - Especifique as opções de configuração do VDA conforme descrito em Instalar usando a linha de comando. As opções `/quiet` e `/noreboot` são incluídas por padrão no script e são obrigatórias: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`.
3. Usando Scripts de Inicialização de Política de Grupo, atribua o script à UO que contém suas máquinas. Esta UO deve conter apenas máquinas nas quais você deseja instalar o VDA. Quando as máquinas nessa UO são reiniciadas, o script é executado em todas elas. Um VDA é instalado em cada máquina que possui um sistema operacional compatível.

### Remover VDAs usando o script

1. Obtenha o script de exemplo UninstallVDA.bat de `\Support\AdDeploy\` na mídia de instalação. A Citrix recomenda que você faça um backup do script original antes de personalizá-lo.
2. Edite o script.
   - Especifique a versão do VDA a ser removida: `SET CHECK\_VDA\_VERSION`. O valor completo pode ser encontrado na mídia de instalação no arquivo ProductVersion.txt (como 7.0.0.3018). No entanto, uma correspondência completa não é necessária.
   - Opcionalmente, especifique um local de compartilhamento de rede para armazenar logs centralizados.
3. Usando Scripts de Inicialização de Política de Grupo, atribua o script à UO que contém suas máquinas. Esta UO deve conter apenas máquinas das quais você deseja remover o VDA. Quando as máquinas na UO são reiniciadas, o script é executado em todas elas. O VDA é removido de cada máquina.

### Solução de problemas

- O script gera arquivos de log internos que descrevem o progresso da execução do script. O script copia um log `Kickoff_VDA_Startup_Script` para o compartilhamento de log central em segundos após o início da implantação. Você pode verificar se o processo geral está funcionando. Se este log não for copiado para o compartilhamento de log central conforme o esperado, solucione o problema inspecionando a máquina local. O script coloca dois arquivos de log de depuração na pasta `%temp%` em cada máquina:
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Revise esses logs para garantir que o script esteja:
  - Executando conforme o esperado.
  - Detectando corretamente o sistema operacional de destino.
  - Corretamente configurado para apontar para o `ROOT` do compartilhamento `DEPLOYSHARE` (contém o arquivo chamado `AutoSelect.exe`).
  - Capaz de autenticar-se nos compartilhamentos `DEPLOYSHARE` e `LOG`.
- Para obter informações sobre como a Citrix relata o resultado das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.

- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA Instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição de programas e recursos da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou um desktop aos usuários até que ele se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro do VDA e como solucionar problemas de registro, consulte Registro do VDA.

# Métodos de implantação de VDA de terceiros

## Instalar VDAs usando Ansible

### Visão geral

Este artigo descreve como implantar VDAs usando Ansible. Para obter mais informações, consulte a documentação Ansible.

> **Nota:**
>
> Este artigo descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

### Etapas principais para implantar VDA usando Ansible

1. Configurar o ambiente da máquina virtual.
2. Instalar o Ansible
3. Configuração do Kerberos
   a. Instalar o Kerberos
   b. Configurar o Kerberos
4. Configurar o Ansible

#### ETAPA 1: CONFIGURAR O AMBIENTE DA MÁQUINA VIRTUAL

Execute os seguintes comandos no servidor Windows.

1. Defina PS RemoteSigned. `Set-ExecutionPolicy RemoteSigned`

2. Defina o WinRM para usar não criptografado: `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

> **Observação:**
>
> Se ocorrer um erro nesta etapa, use o seguinte comando: `Enable-PSRemoting -Force`

3. Abra a porta 5985 do firewall. `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

### ETAPA 2: INSTALAR O ANSIBLE

Para instalar o Ansible com Ubuntu 20.4 ou posterior, execute os seguintes comandos:

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

### ETAPA 2I: INSTALAR O KERBEROS

Para instalar o Kerberos, execute o seguinte comando.

`sudo apt install python3-dev libkrb5-dev krb5-user`

### ETAPA 2II: CONFIGURAR O KERBEROS

Para configurar o Kerberos, execute o seguinte comando:

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

**Nota:**

Use letras maiúsculas para o nome do realm do Kerberos.

```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        .toronto.edu = UTORONTO.CA
        .utoronto.ca = UTORONTO.CA
```

### ETAPA 3: CONFIGURAR O ANSIBLE

Para configurar o host do Ansible, conclua as seguintes etapas:

1. Execute o seguinte comando:

   `Edit /etc/ansible/hosts`

2. Configure um arquivo `Install.yaml` do Controlador de Entrega

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

```
- name: Install multi-session VDA using network share path
  hosts: TSVDA

  tasks:

  - name: mount a cvad iso
    community.windows.win_disk_image:
      image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: present
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user: [redacted]
      ansible_become_password: [redacted]
    register: disk_image_out

  - name: copy iso file to c drive temp folder
    ansible.windows.win_copy:
      src: "{{disk_image_out.mount_paths[0]}}"
      dest: C:\Temp\
      remote_src: yes

  - name: unmount iso
    community.windows.win_disk_image:
      image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: absent
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user: [redacted]
      ansible_become_password: [redacted]
-- INSERT --                                                                    26,83         Top
```

```
- name: unmount iso
  community.windows.win_disk_image:
    image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
    state: absent
  become: true
  become_method: runas
  become_flags: logon_type=new_credentials logon_flags=netcredentials_only
  vars:
    ansible_become_user: [redacted]
    ansible_become_password: [redacted]

- name: stop windows upgrade service
  ansible.windows.win_service:
    name: wuauserv
    start_mode: disabled
    state: stopped

- name: Restart server before install
  ansible.windows.win_reboot:

- name: Install vda from exe
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    arguments: /quiet /verboselog /PORTNUMBER [redacted] /logpath 'C:\CitrixInstallationLogs\TSVDA' /components "VDA,PLUGINS"  /CONT
ROLLERS '[redacted]'  /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT /NOREBOOT /NORESUME
    expected_return_code: [0, 3,3010]
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
```

```
    register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
  win_reboot:
  when: install_vda.changed

- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find
```

```
- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find

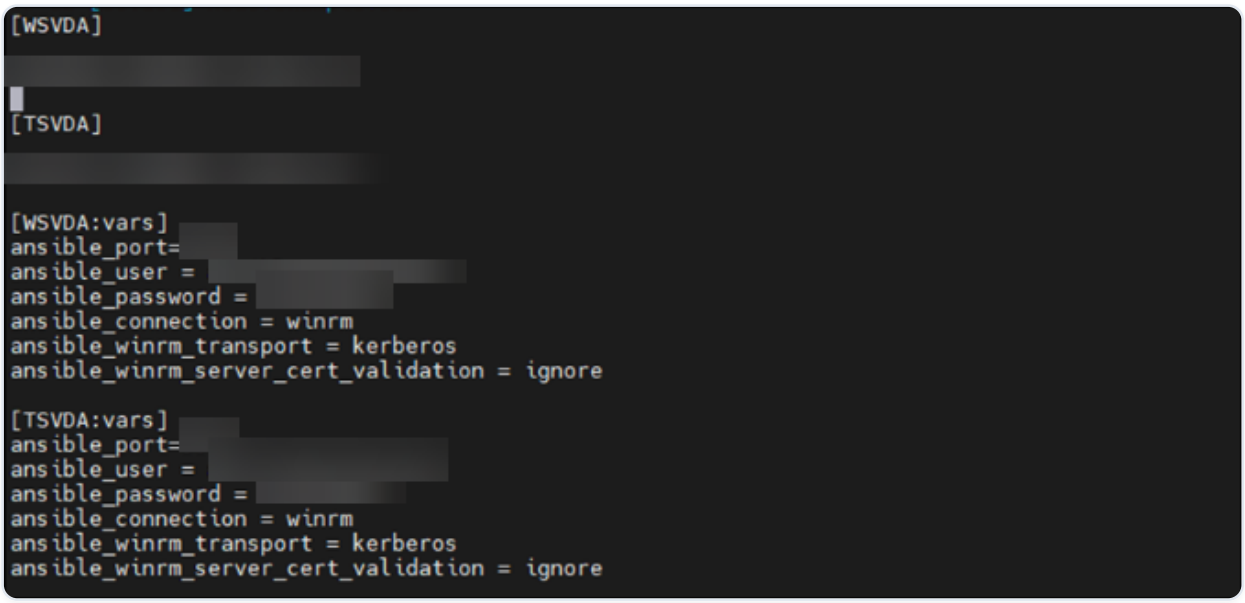
- name: Restart server after VDA install
  win_reboot:
  when: vda_install_find.matched == 0

- name: remove temp folder
  win_file:
    path: C:\Temp\
    state: absent
```

1. Execute o arquivo yaml com o seguinte comando: `sudo ansible-playbook install.yml -vvv` (Modo detalhado)

2. Você pode configurar vários hosts no arquivo de configuração com outras configurações adicionais.

   `Edit /etc/ansible/hosts`




## Instalar VDAs usando o Microsoft Intune

### Visão geral

Este artigo descreve como implantar VDAs usando o Microsoft Intune. Para mais informações, consulte a documentação Microsoft.

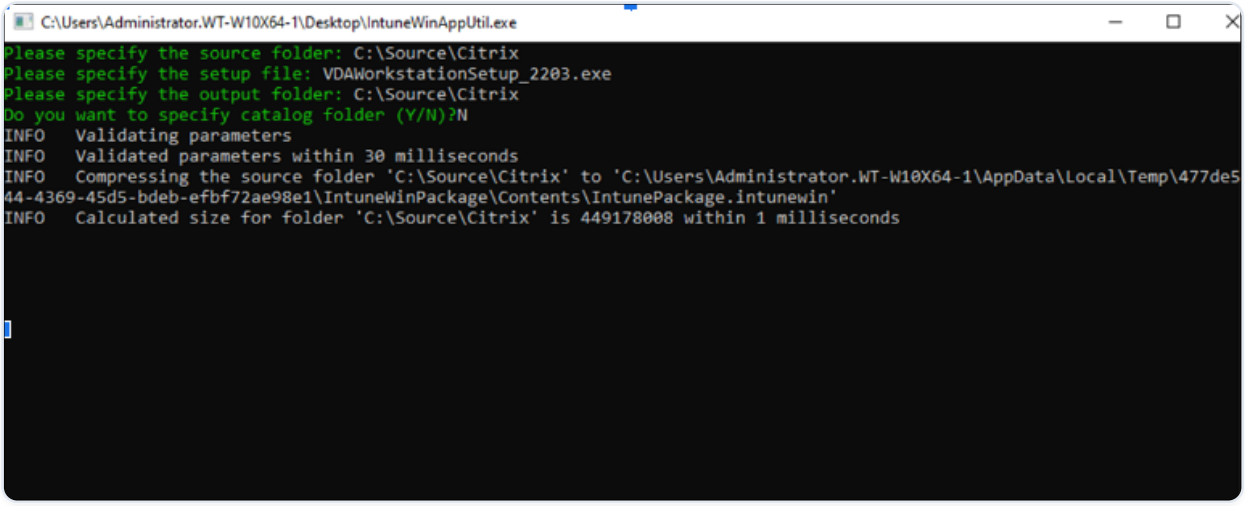
> **Nota:**
>
> O artigo a seguir descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

### Etapas principais para implantar VDA usando o Microsoft Intune

1. Preparar a instalação para o VDA Citrix.
2. Configurar o Assinante do Programa de Desenvolvedores do Microsoft 365.
3. Adicionar e atribuir um aplicativo.
4. Instalar o aplicativo no dispositivo registrado.

### ETAPA 1: PREPARAR A INSTALAÇÃO PARA O CITRIX VDA

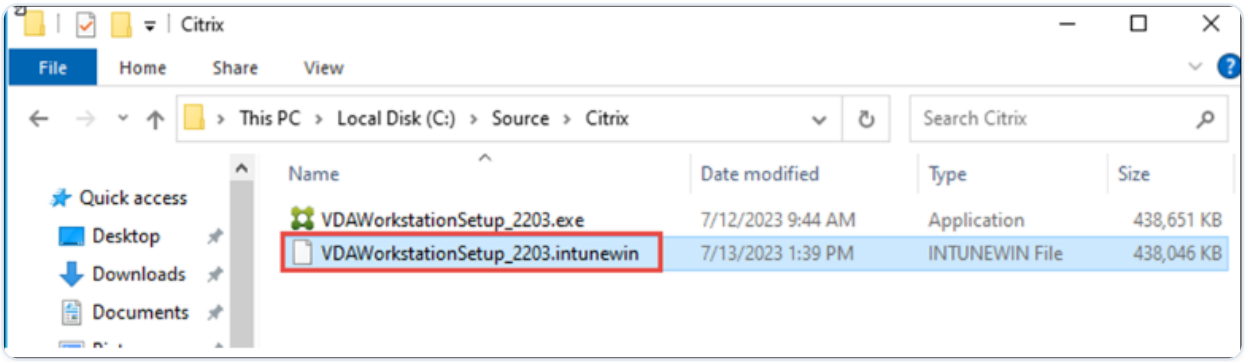
1. Baixe o IntuneWinAppUtil.exe atualizado do GitHub.
2. Execute o arquivo `IntuneWinAppUtil.exe` usando **Executar como administrador**.
3. Insira os seguintes dados:




   a. **Especifique a pasta de origem**: Insira a pasta que contém os arquivos de configuração do seu aplicativo. Por exemplo, C:\source\Citrix.
   b. **Especifique o arquivo de configuração**: Insira o nome do arquivo de configuração (como setup.exe ou setup.msi). Por exemplo, VDAWorkstationSetup_2203.exe.
   c. **Por favor, especifique a pasta de saída**: Insira o caminho da pasta de saída para gerar o arquivo .intunewin. Por exemplo, C:\source\Citrix.
   d. **Deseja especificar a pasta de catálogo (S/N)**: Digite N.

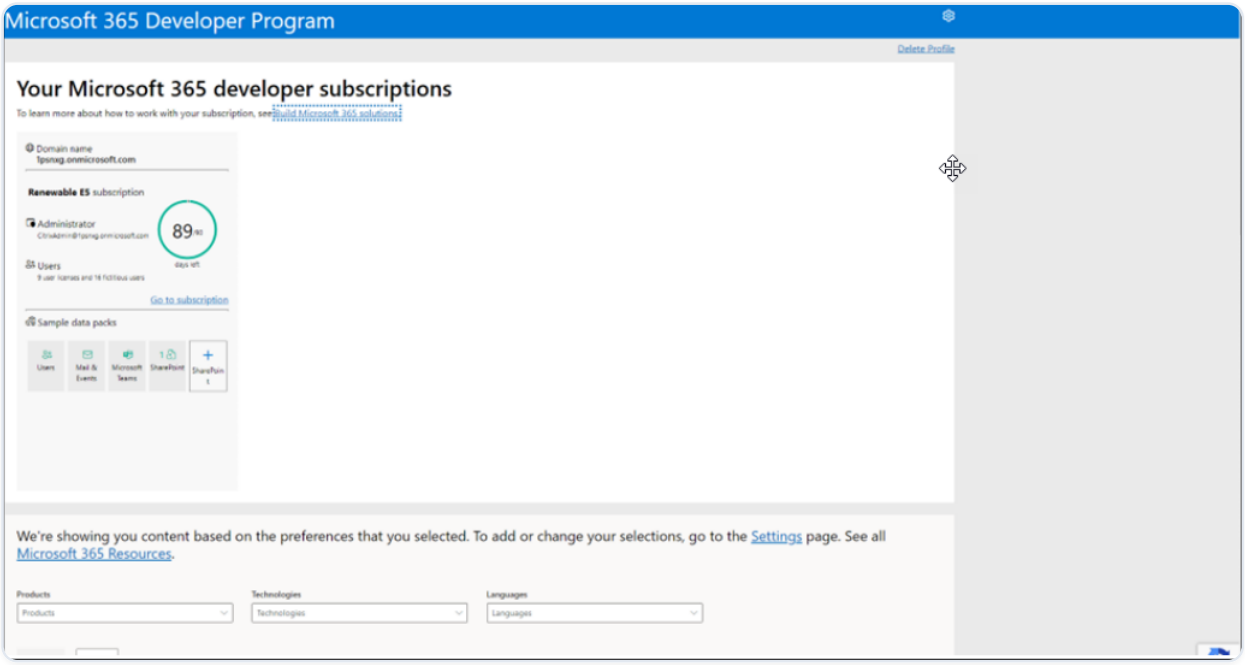
> **Nota:**
>
> Espere alguns minutos enquanto a **Win32 Content Prep Tool** está em execução. Assim que ela gerar o arquivo `.intunewin`, o status indicará 100% na parte inferior do prompt de comando.

4. Assim que o processo for concluído, vá para a pasta de saída (neste exemplo, `C:\source\Citrix`) para obter o arquivo de implantação do Microsoft Intune.
5. Inscreva-se para uma avaliação gratuita do Microsoft Intune.

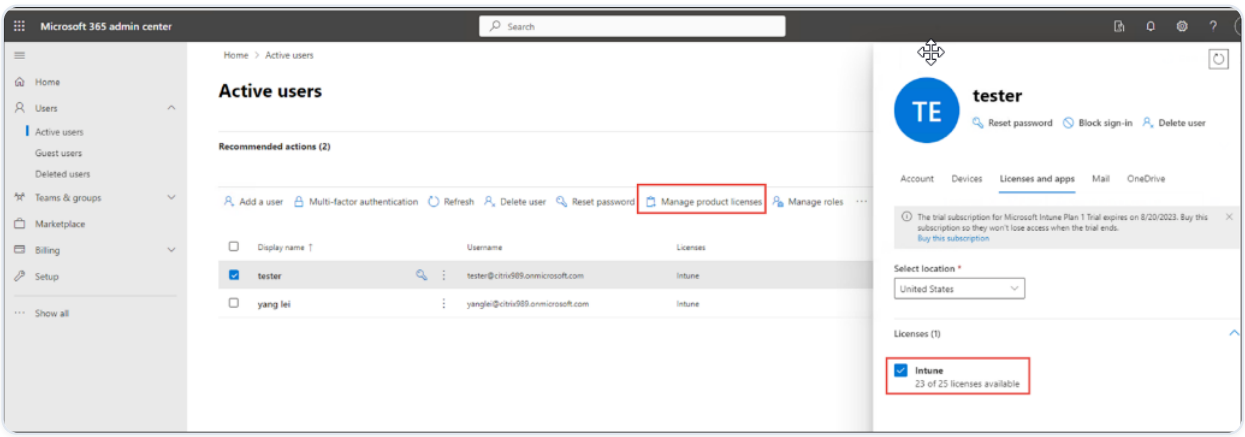



## ETAPA 2: CONFIGURAR O ASSINANTE DO PROGRAMA DE DESENVOLVEDORES DO MICROSOFT 365

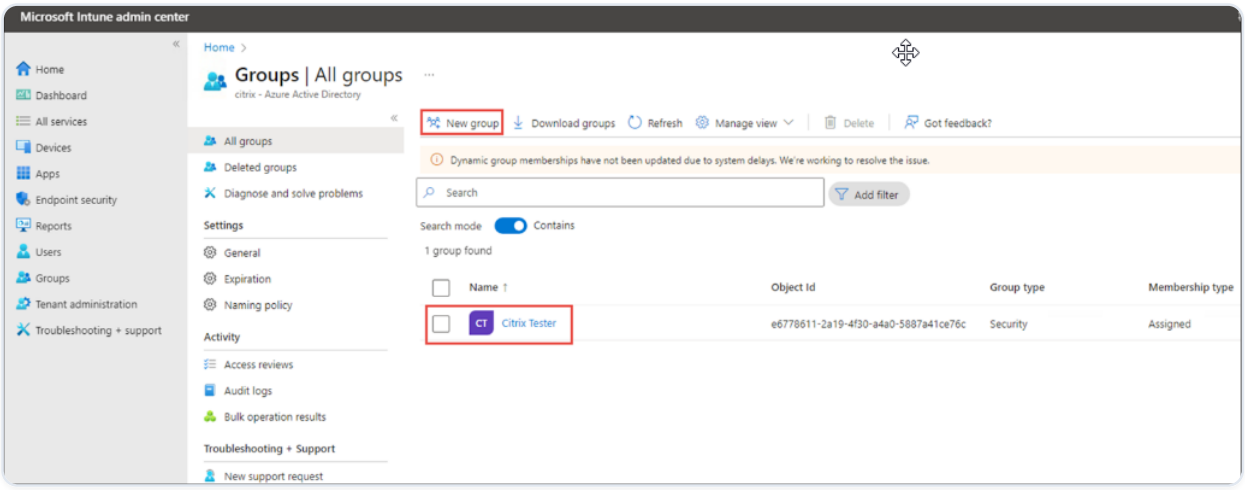
1. Crie o sandbox instantâneo para ativar sua assinatura. Para obter seu sandbox de desenvolvedor, vá para o seu painel do Programa de Desenvolvedores do Microsoft 365 e selecione **Adicionar uma nova assinatura**.




2. Crie um usuário no centro de administração do Microsoft 365 e atribua uma licença ao usuário.




3. Crie um grupo.




4. Depois que o grupo for criado, você deve fornecer a autoridade MDM ao grupo. Configure o registro automático. Pode levar um minuto para ativar. Ou você pode adicionar manualmente a autoridade MDM ao grupo, seguindo estas etapas:

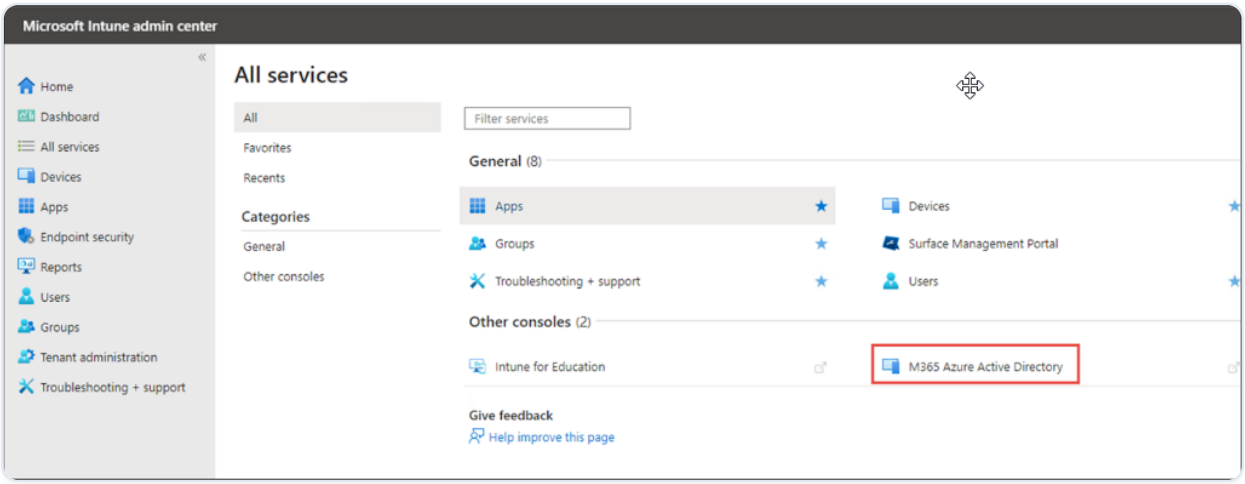
   a. Vá para **Todos os serviços > Microsoft Entra**.

   b. Vá para **configurações > Mobilidade** e selecione **Microsoft Intune**.

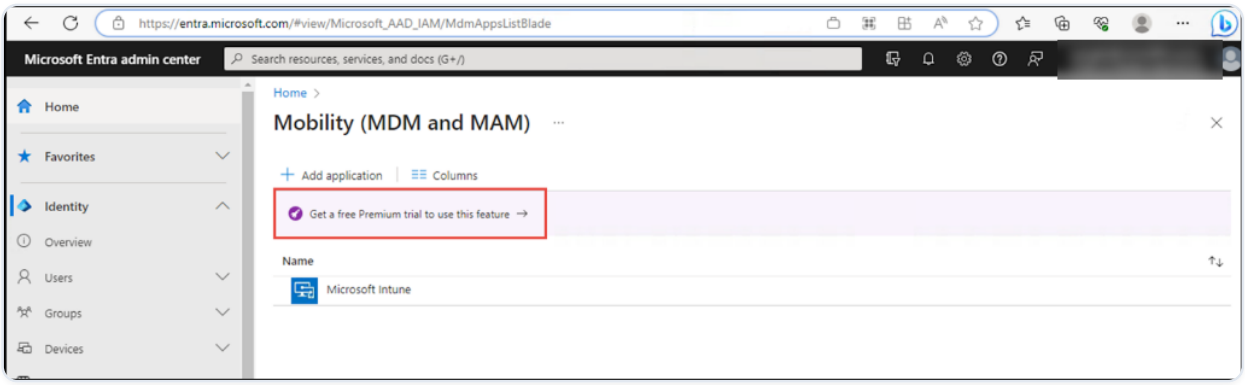
   c. Selecione o grupo que você acabou de criar. Isso abre uma página com o escopo de usuário MDM.

   d. Clique em **Salvar**.

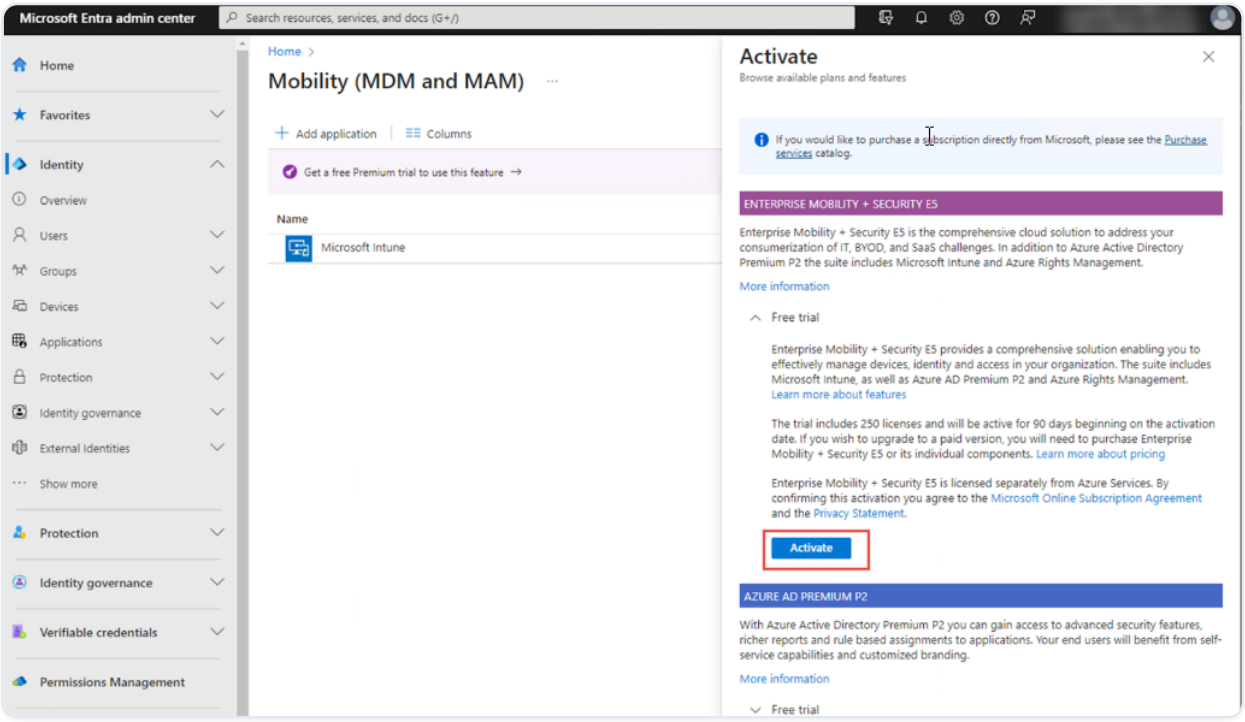
5. Na guia **Todos os Serviços**, clique em **M365 Azure Active Directory**.



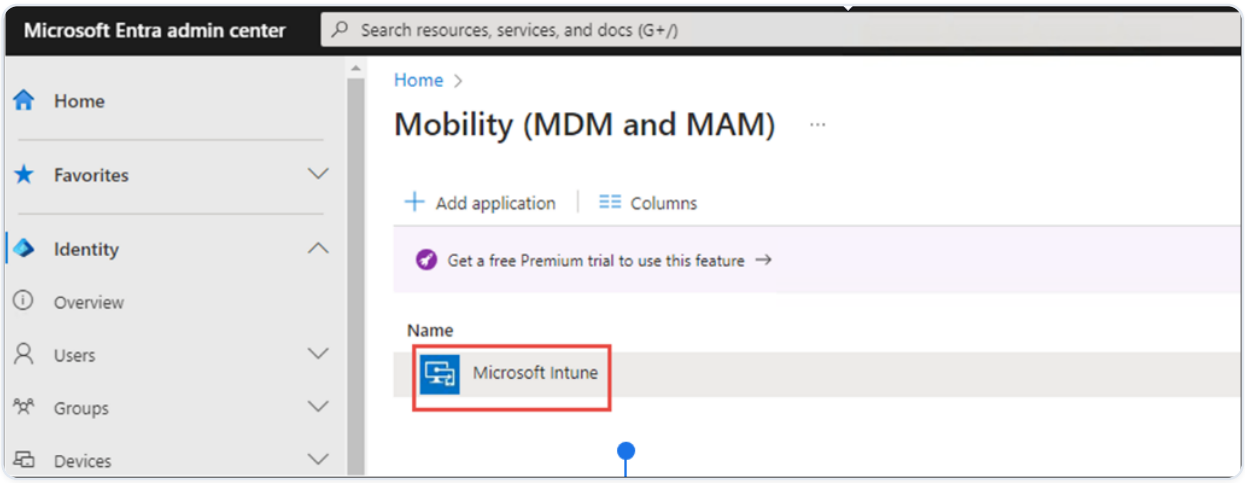
6. Clique em **Obter uma avaliação Premium gratuita para usar este recurso**.



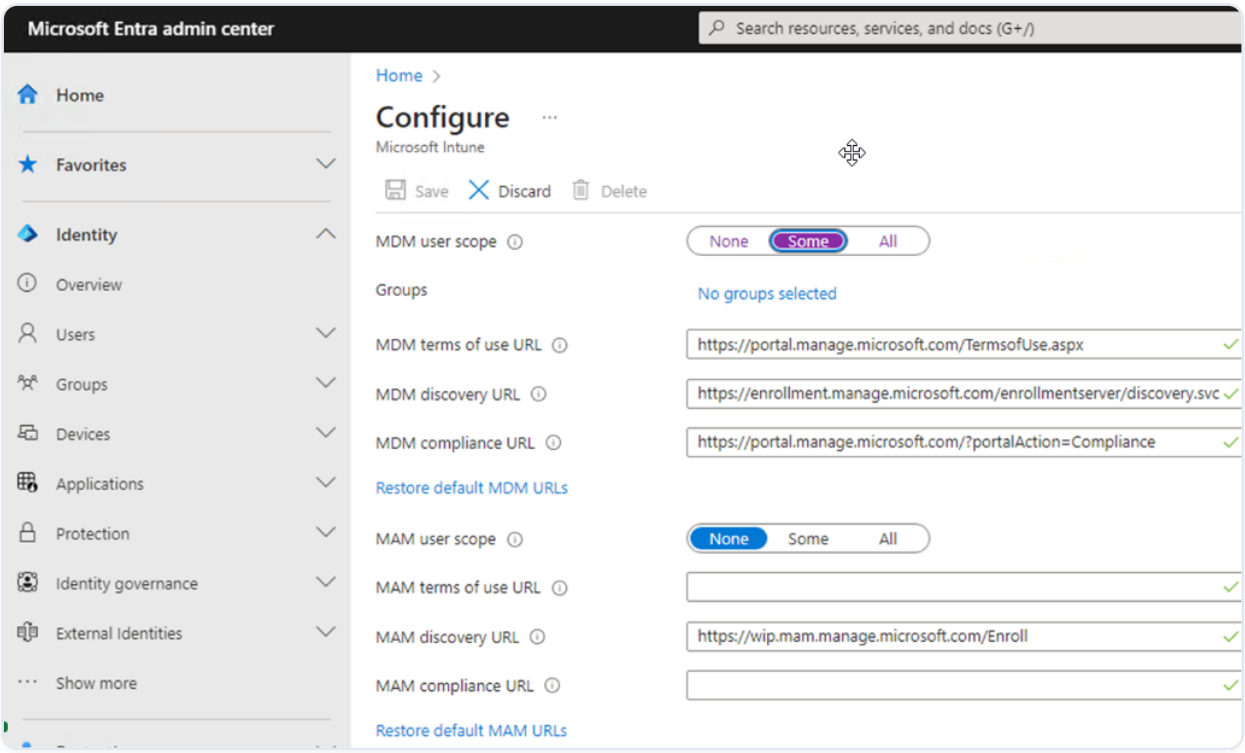

7. Clique em **Ativar**.



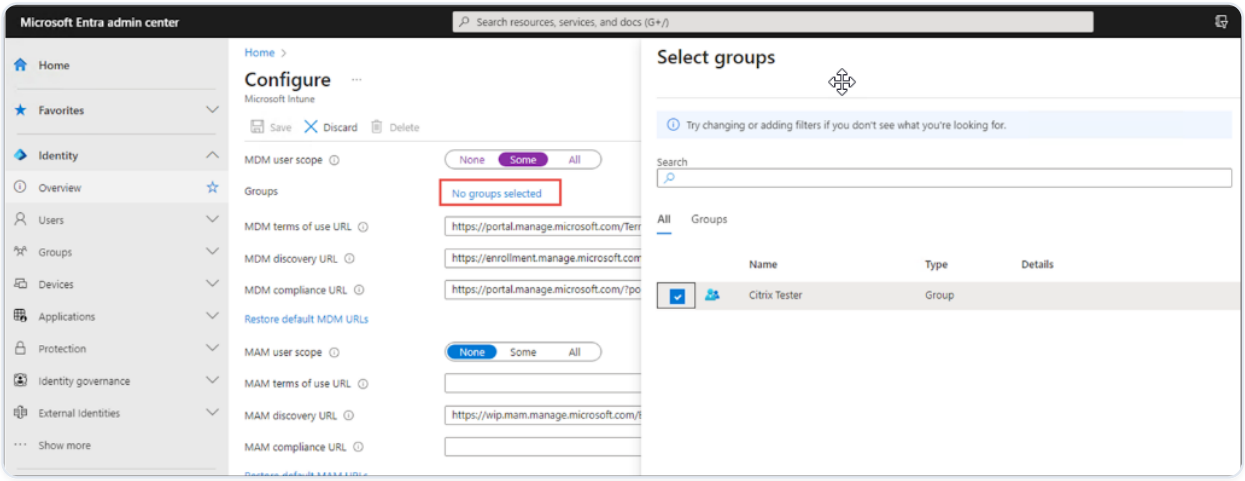

8. Agora, clique em **Microsoft Intune**.



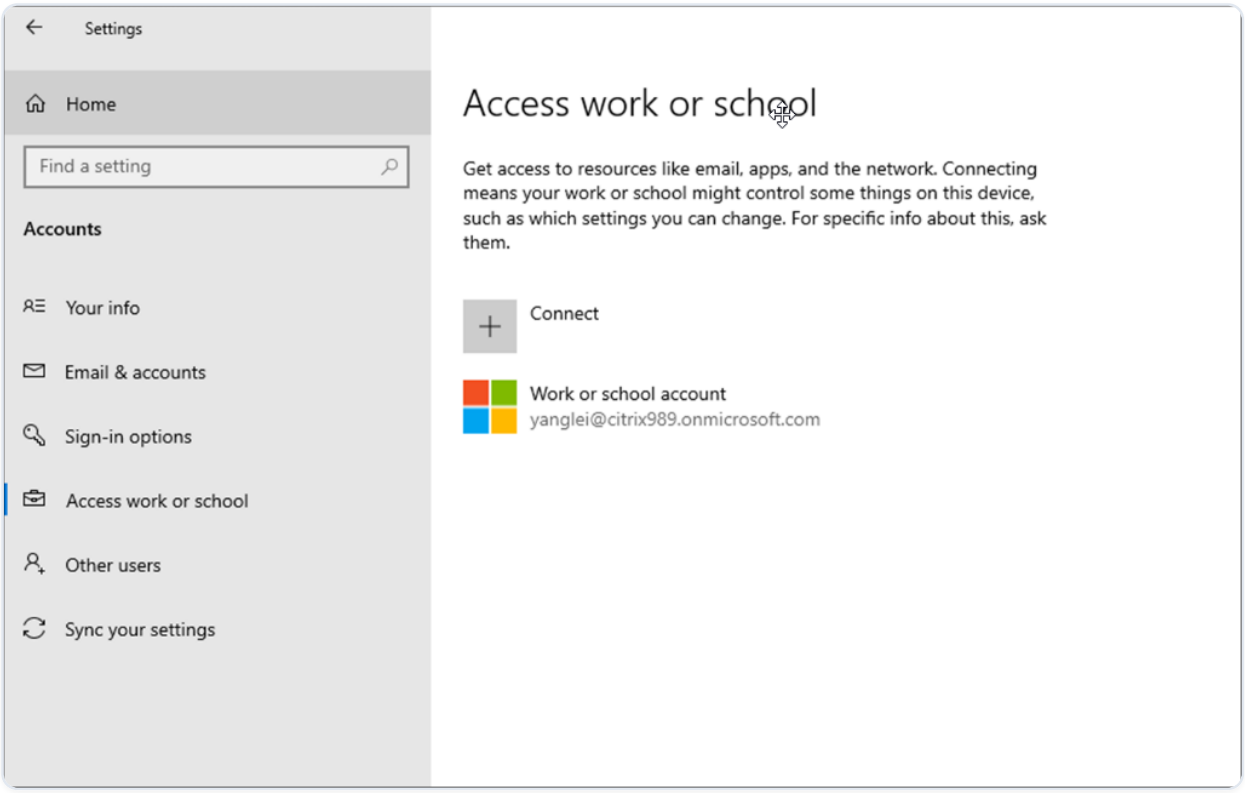

9. Na guia **Configurar**, insira as configurações necessárias.



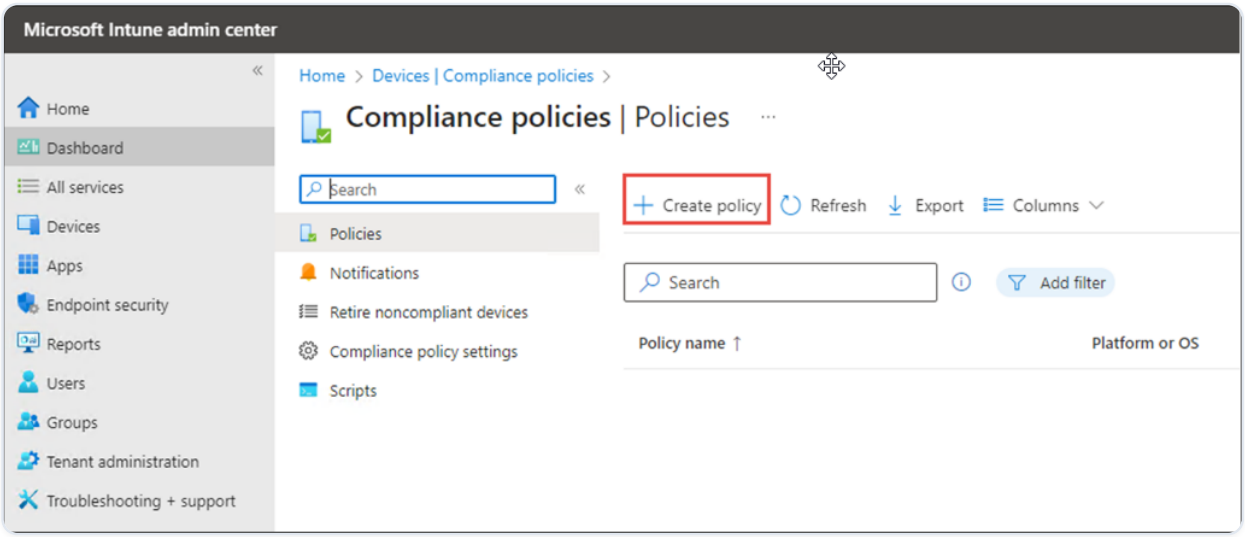

10. Para adicionar um grupo, clique em **Nenhum grupo selecionado**.



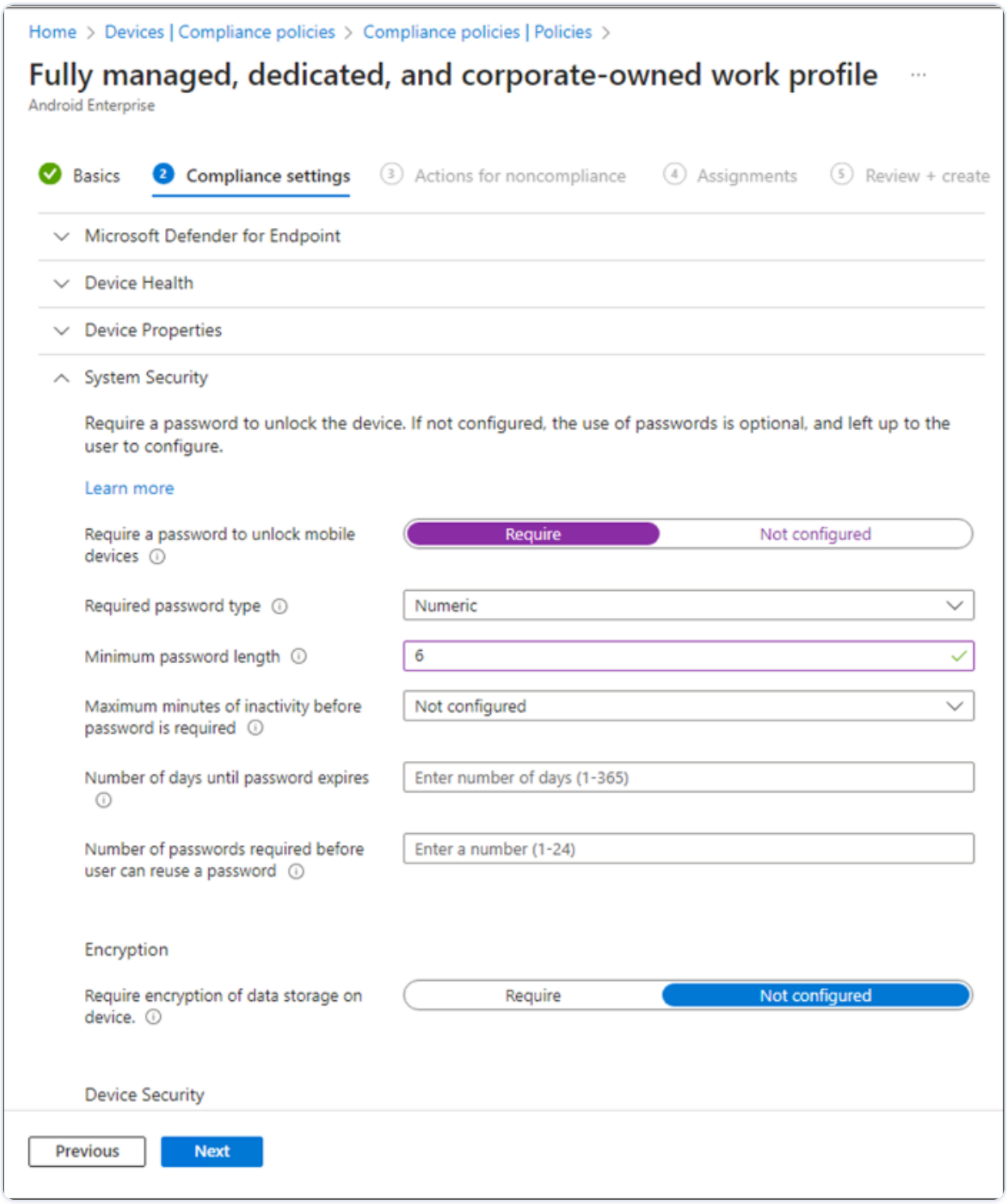

11. Registre seu dispositivo.



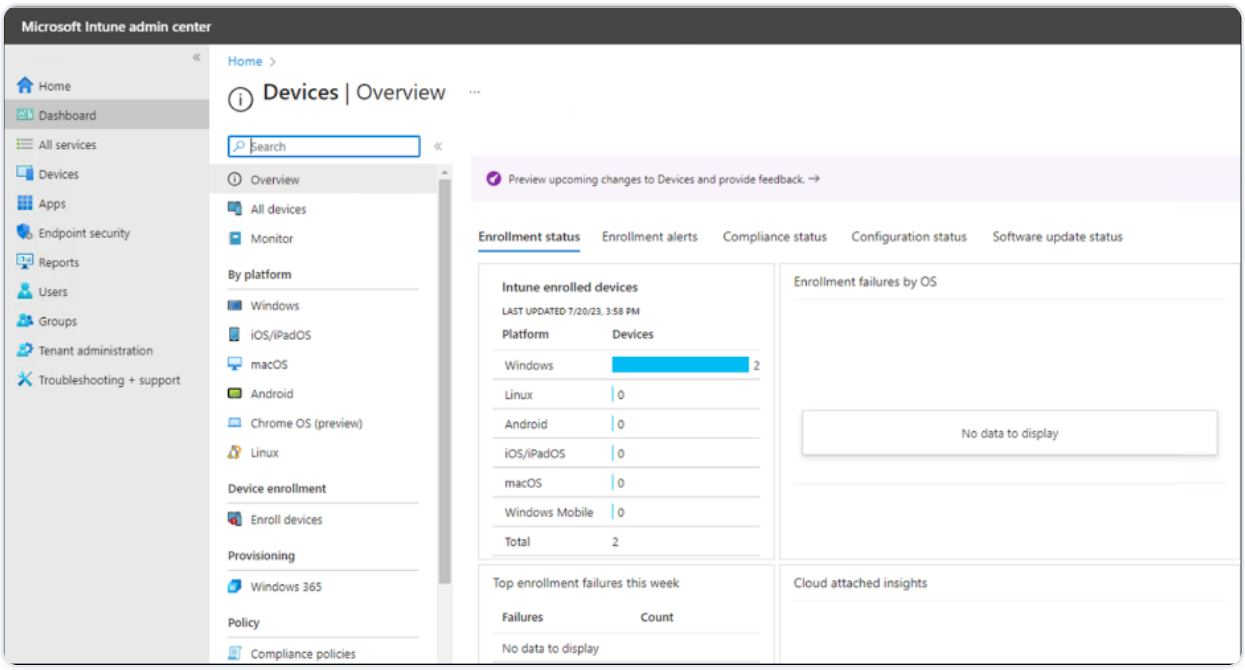

12. Crie uma política de conformidade de dispositivo para alterar a conformidade do seu dispositivo recém-criado para `Compliant`.




13. Vá para a guia **Atribuições** para adicionar o grupo recém-criado.



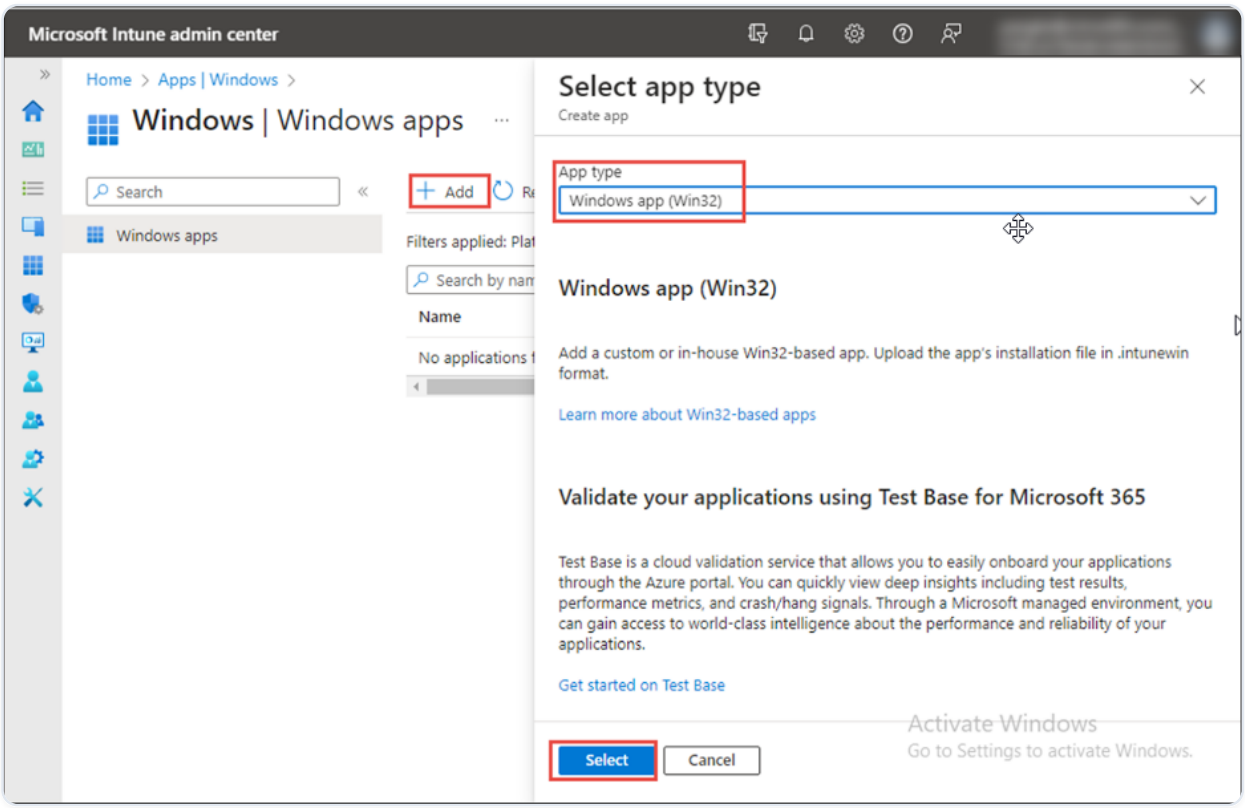

14. Confirme o registro do dispositivo.



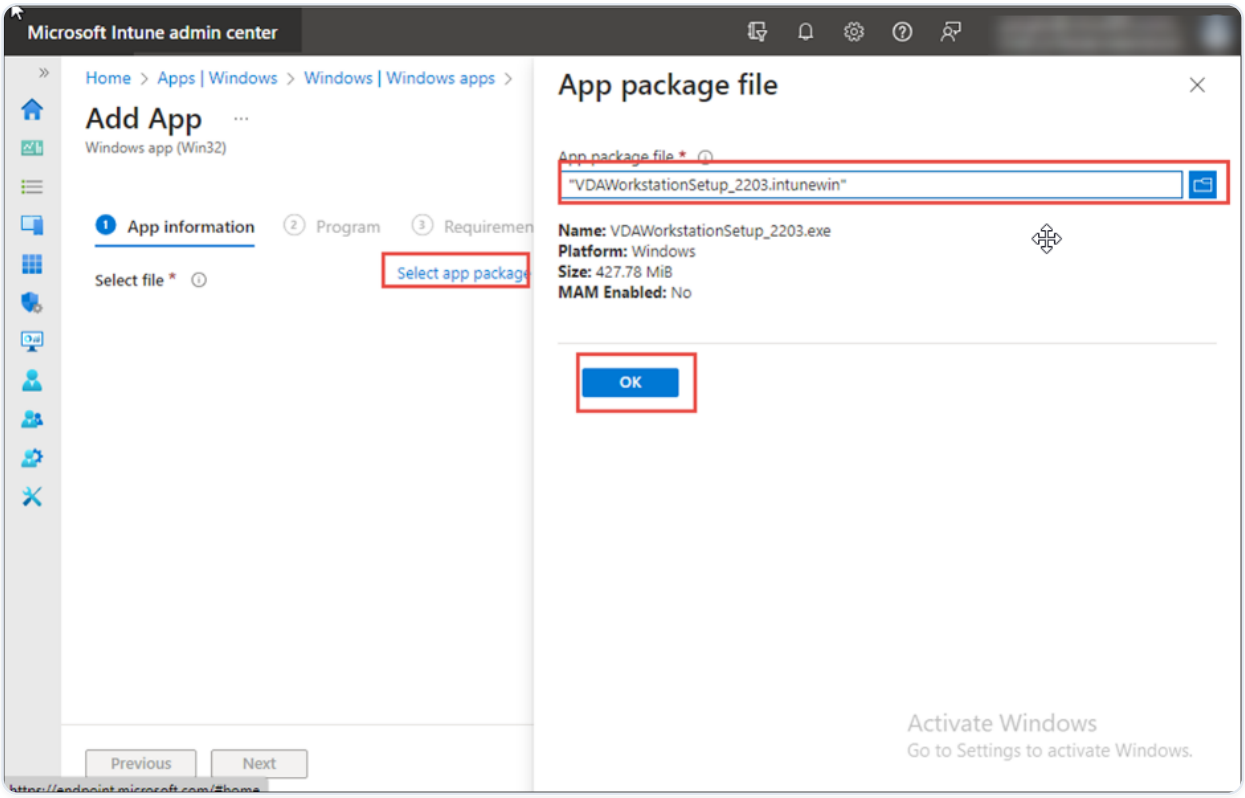

Para obter informações detalhadas, consulte programa de desenvolvedor do Microsoft 365.

### ETAPA 3: ADICIONAR E ATRIBUIR UM APLICATIVO

1. Faça login no centro de administração do Microsoft Intune.
2. Selecione **Aplicativos > Todos os aplicativos > Adicionar** ou vá para **Aplicativos > Windows > Aplicativos do Windows**.



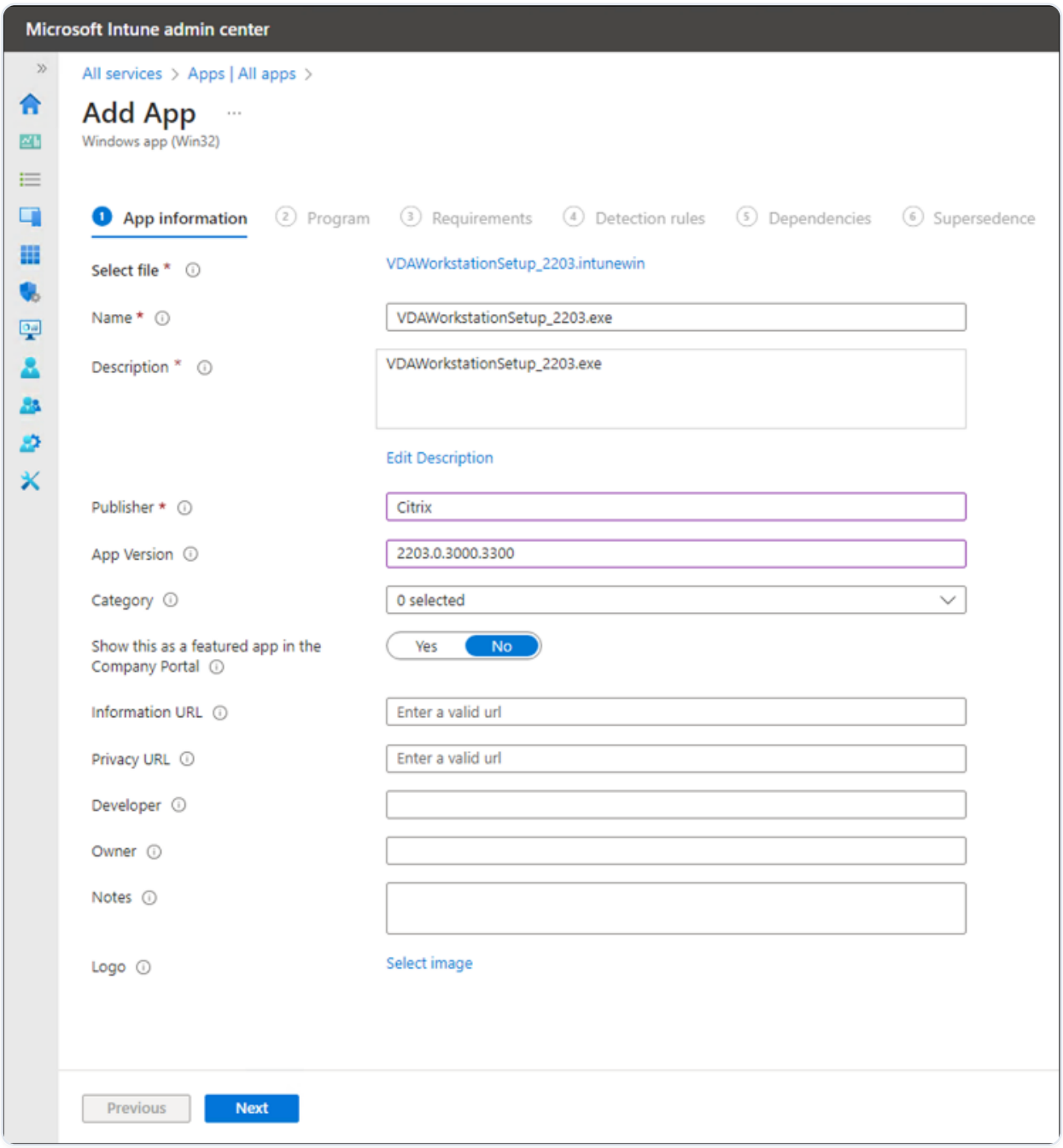
3. No painel **Selecionar tipo de aplicativo**, selecione **Outros tipos de aplicativo > Aplicativo Windows (Win32)** e clique em **Selecionar**.
4. No painel **Adicionar aplicativo**, clique em **Selecionar arquivo de pacote de aplicativo**. Clique em **procurar**.
5. Selecione o arquivo preparado com a extensão `.intunewin`. O arquivo preparado é criado durante a etapa Preparar a instalação para o Citrix VDA. Uma página contendo informações detalhadas sobre o aplicativo é exibida.




**Nota:**

- Se você estiver usando uma máquina server-core, você deve usar o VDA workstation core.
- Se você estiver usando um sistema operacional de desktop Windows 10, você deve usar o VDA workstation.
- Se você estiver usando um sistema operacional de servidor (Por exemplo, Windows 2022), você deve usar a configuração do VDA server.
- Neste exemplo, estamos usando a versão 2203, mas isso é aplicável a todas as versões.

6. Clique em **OK** no painel **Arquivo de pacote do aplicativo**.
7. Na tela seguinte, na guia **Informações do Aplicativo**, insira o **Nome** do Aplicativo e a **Descrição** do Aplicativo Windows. Insira o nome do **Editor** como `Citrix`, e você pode especificar as informações adicionais do aplicativo aqui. Clique em **Avançar**.




8. Na próxima tela, insira os seguintes valores:

   - **Comando de instalação**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **Comando de desinstalação**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **Comportamento de instalação**:

- **Sistema**: Selecione esta opção para instalar o aplicativo em todos os dispositivos do grupo.
- **Usuário**: Selecione esta opção para instalar o aplicativo apenas em um dispositivo de usuário específico no grupo.

9. Clique em **Avançar**.

> **Nota:**
>
> - Este exemplo usa a versão 2203, mas você pode usá-lo com qualquer versão.
> - Adicionar `/noreboot` a um comando não significa que não haverá reinicializações durante a instalação ou implantação, mas apenas impõe reinicializações obrigatórias. Para obter mais informações sobre scripts, consulte Opções de linha de comando para instalar um VDA.
> - Para **Comportamento de reinício do dispositivo**, selecione **O Intune forçará um reinício obrigatório do dispositivo**.
> - Na caixa de texto **Código de retorno**, insira `0`, `3` e `8` para sucesso pós-instalação. Para obter informações sobre outros códigos de retorno, consulte Códigos de retorno de instalação do Citrix.

> Intune adicionar aplicativo(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/intune-add-app-2.png)

10. Na tela a seguir, na guia **Requisitos**, insira os valores necessários. Clique em **Avançar**.

    Intune adicionar aplicativo(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/intune-add-app-req.png)

11. Na tela a seguir, na guia **Regra de detecção**, adicione **Regra de detecção** para adicionar o agente Broker. Clique em **OK**.

    Regra de detecção(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/intune-detection-rule.png)

12. Na guia **Atribuições**, você pode adicionar os dispositivos da seguinte forma:

    - **Obrigatório**: Os dispositivos para os quais as atualizações ocorrem automaticamente.

- **Disponível para dispositivos registrados**: Os dispositivos para os quais as atualizações ocorrem manualmente.

Adicionar mais aplicativos(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/intune-add-app-more.png)

13. Revise os detalhes e clique em **Criar**.

    Centro de administração(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/ms-intune-admin-center-3.png)

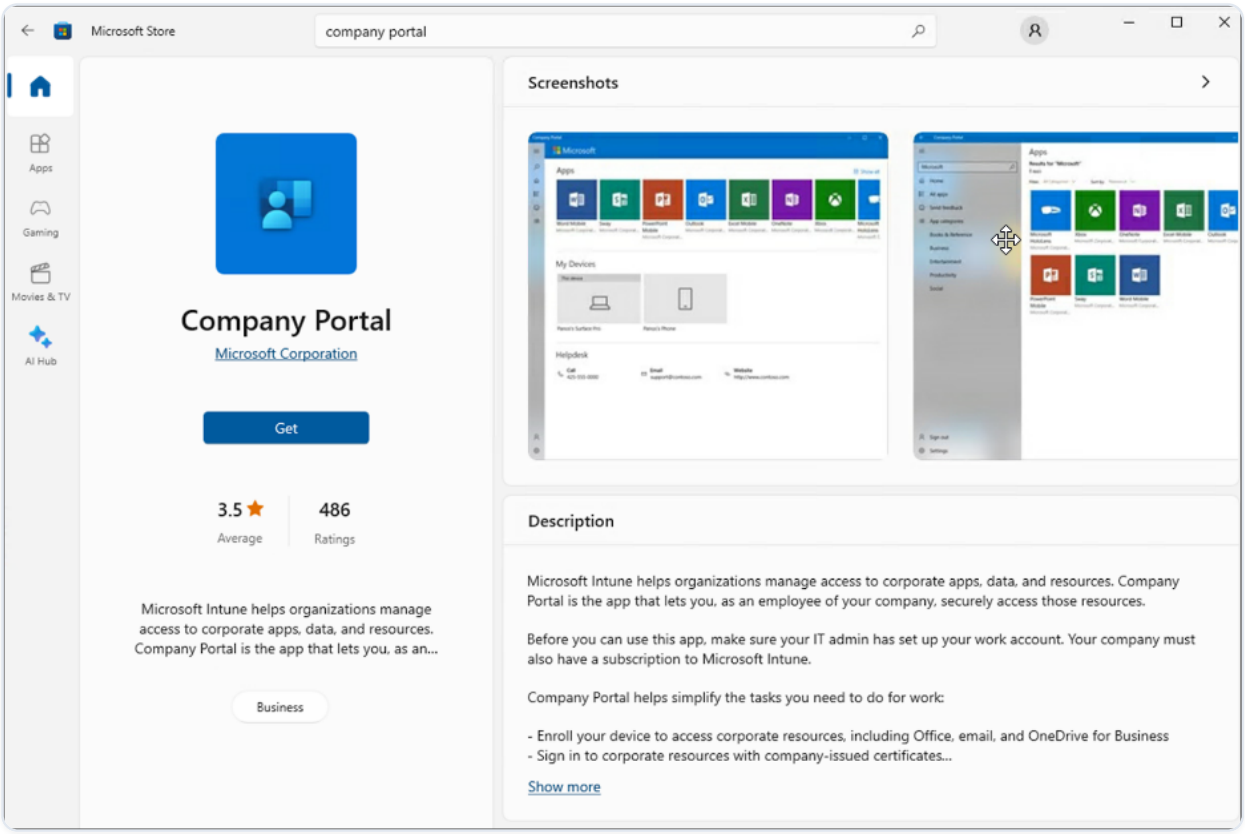
    O aplicativo foi atribuído com sucesso.

    Aplicativo atribuído(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/intune-vda-creation.png)

Para informações detalhadas, consulte Adicionar e atribuir um aplicativo.

### ETAPA 4: INSTALAR O APLICATIVO NO DISPOSITIVO REGISTRADO

1. Faça login no seu dispositivo Windows 10 Desktop registrado. O dispositivo deve estar registrado no Microsoft Intune. Além disso, você deve fazer login no dispositivo usando uma conta contida no grupo que você atribuiu ao aplicativo. Para obter mais informações, consulte a documentação da Microsoft.
2. No menu **Iniciar**, abra a **Microsoft Store**.
3. Procure o aplicativo **Portal da Empresa** e instale-o.




4. Execute o aplicativo **Portal da Empresa**.
5. Clique no aplicativo que você adicionou usando o Microsoft Intune. Se você não atribuiu nenhum aplicativo com sucesso ao usuário do Intune, a seguinte mensagem será exibida: `Your IT administrator did not make any apps available to you.`
6. Clique em **Instalar**.

# Criar um site

> **Nota:**
>
> Durante a criação do site, depois de adicionar uma licença para habilitar a Licença de Direitos Híbridos, os hosts de nuvem pública (como Microsoft Azure, Google Cloud Platform e Amazon Web Services) não aparecem na lista de tipos de conexão até que a criação do site seja concluída.

Um site é o nome que você dá a uma implantação do Citrix Virtual Apps and Desktops™. Ele compreende os Delivery Controllers e outros componentes principais, Virtual Delivery Agents (VDAs), conexões com hosts, catálogos de máquinas e grupos de entrega. Você cria o site

> depois de instalar os componentes principais e antes de criar o primeiro catálogo de máquinas e grupo de entrega.

Se o seu Controller estiver instalado no Server Core, use os cmdlets do PowerShell no Citrix Virtual Apps and Desktops SDK para criar um site.

Ao criar um site, você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix. O CEIP coleta estatísticas anônimas e informações de uso e as envia para a Citrix. O primeiro pacote de dados é enviado para a Citrix aproximadamente sete dias após a criação do site. Você pode alterar sua inscrição a qualquer momento após a criação do site. Selecione **Configurações** no painel esquerdo do Web Studio e, em seguida, localize a configuração **Programa de Melhoria da Experiência do Cliente da Citrix**. Para obter detalhes, consulte `<http://more.citrix.com/XD-CEIP>`.

O usuário que cria um site se torna um administrador completo. Para obter mais informações, consulte Administração delegada.

Revise este artigo antes de criar o site, para saber o que esperar.

## Etapa 1. Abra o assistente de criação de site - Citrix Site Manager

Use a ferramenta Citrix Site Manager para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como site). A ferramenta é instalada automaticamente quando você instala um Delivery Controller.

Para executar esta ferramenta, abra o menu Iniciar da sua área de trabalho em um Delivery Controller e selecione **Citrix > Citrix Site Manager**. Consulte Instalar o Web Studio.

## Etapa 2. Nome do site

Na página **Introdução**, digite um nome para o site.

## Etapa 3. Bancos de dados

A página **Bancos de dados** contém seleções para configurar o site, monitoramento e bancos de dados de registro de configuração. Para obter detalhes sobre as opções e requisitos de configuração do banco de dados, consulte Bancos de dados.

> **Nota:**

> Se um SQL Server Always On Listener estiver configurado para criptografia TLS, você poderá ser solicitado a inserir credenciais com permissões de criação de banco de dados. As tentativas de criar o banco de dados ainda falharão mesmo se você inserir credenciais de administrador válidas. Verifique se o certificado do SQL Server inclui o nome DNS do listener nos Nomes Alternativos do Assunto (SAN). Para obter mais informações, consulte `<https://docs.microsoft.com/pt-br/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>`.

> Se você optar por instalar o SQL Server Express para usar como banco de dados do site (o padrão), ocorre uma reinicialização após a instalação desse software. Essa reinicialização não ocorre se você optar por não instalar o software SQL Server Express para usar como banco de dados do site.

Se você não estiver usando o SQL Server Express padrão, certifique-se de que o software SQL Server esteja instalado nas máquinas antes de criar um site. Requisitos do sistema lista as versões suportadas.

Se você quiser adicionar mais Delivery Controllers ao site, e já tiver instalado o software Controller em outros servidores, você pode adicionar esses Controllers a partir desta página. Se você também planeja gerar scripts que configuram os bancos de dados, adicione os Controllers antes de gerar os scripts.

## Etapa 4. Licenciamento

> **Nota:**

> Certifique-se de que o License Server esteja executando no mínimo a versão 11.17.2 build 53100 ou superior. O não cumprimento deste pré-requisito pode causar erros ou recomendações durante as atualizações e a criação do site.

> Na página **Licenciamento**, especifique o endereço do License Server e, em seguida, indique qual licença usar (instalar).

- Especifique o endereço do License Server no formato `name:[port]`. O *nome* deve ser um FQDN, NetBIOS ou endereço IP. FQDN é recomendado. Se você omitir o número da porta, o padrão é 27000. Clique em **Conectar**. Você não pode prosseguir para a próxima página até que uma conexão bem-sucedida seja feita com o License Server.

- Quando uma conexão é estabelecida, **Usar uma licença existente** é selecionado por padrão. A exibição lista os produtos compatíveis para os quais este produto pode ser configurado, com base nas licenças atualmente instaladas.
  - Se você quiser configurar este produto como um dos produtos listados (por exemplo, Citrix Virtual Apps Premium ou Citrix Virtual Desktops™ Premium), usando uma dessas licenças, selecione essa entrada.
  - Se você já alocou e baixou uma licença (usando a Ferramenta Citrix Manage Licenses) para usar com este produto, mas ainda não instalou a licença:
    - Clique em **Procurar arquivo de licença**.
    - No explorador de arquivos, localize e selecione a licença que você baixou. Os produtos associados agora aparecem na página **Licenciamento** do assistente de criação do site. Selecione a entrada que deseja usar.
  - Se o produto desejado não for exibido, ou se você não tiver licenças alocadas e baixadas, poderá alocar, baixar e instalar uma licença. Para fazer isso, o License Server deve ter acesso à internet. Você deve ter um Código de Acesso à Licença para o produto desejado. A Citrix envia esse código por e-mail para você.
    - Clique em **Alocar e baixar**.
    - Na caixa de diálogo **Alocar Licenças**, insira o Código de Acesso à Licença enviado pela Citrix. Clique em **Alocar licenças**.
    - Os produtos associados à nova licença aparecem na página **Licenciamento** do assistente de criação do site. Selecione a entrada que deseja usar.

  Alternativamente, selecione **Usar a avaliação gratuita de 30 dias** e instale as licenças mais tarde. Para obter detalhes, consulte a documentação de Licenciamento.

## Etapa 5. Resumo

A página **Resumo** lista as informações que você especificou. Use o botão **Voltar** se quiser alterar algo. Quando terminar, clique em **Concluir**.

## Mais informações

### Conexão de host, rede e armazenamento

Se você estiver usando VMs em um hipervisor ou outro serviço para entregar aplicativos e desktops, poderá, opcionalmente, criar a primeira conexão com esse host. Você também pode

especificar recursos de armazenamento e rede para essa conexão. Após criar o site, você pode modificar esta conexão e recursos, e criar mais conexões. Para obter detalhes, consulte Conexões e recursos.

- Para obter informações especificadas na página **Conexão**, consulte Conexões e recursos.
  - Se você não estiver usando VMs em um hipervisor ou outro serviço (ou se usar o Web Studio para gerenciar desktops em PCs blade dedicados), selecione o tipo de conexão **Nenhum**.
  - Se você estiver configurando um site de Acesso Remoto para PC e planeja usar o recurso Wake on LAN, selecione o tipo **Microsoft System Center Virtual Machine Manager** ou **Remote PC Wake on LAN**. Para obter mais informações, consulte Wake on LAN.

  Além do tipo de conexão, especifique se você usará ferramentas Citrix (como Machine Creation Services™) ou outras ferramentas para criar VMs.
- Para obter informações especificadas nas páginas **Armazenamento** e **Rede**, consulte Armazenamento de host, Gerenciamento de armazenamento e Seleção de armazenamento.
- Se você tiver uma Licença de Direitos Híbridos e tiver adicionado conexões de host de nuvem pública (por exemplo, AWS), essas conexões serão listadas aqui. Para visualizar essas conexões de host de nuvem pública, atualize o Web Studio vários minutos após adicioná-las.

### Acesso Remoto ao PC

Para obter informações sobre implantações de Acesso Remoto para PC, consulte Acesso Remoto para PC.

Se você usar o recurso Wake on LAN, conclua as etapas de configuração no Microsoft System Center Configuration Manager antes de criar o site. Para obter detalhes, consulte Configuration Manager e Acesso Remoto para PC Wake on LAN.

# Criar e gerenciar conexões e recursos

> **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 (EOL) que usam essas tecnologias.

- Personal vDisks (PvDs)
- AppDisks™
- Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic

Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

**Observação:**

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

Se você deseja usar conexões de host de nuvem pública em sua implantação, precisa da Licença de Direitos Híbridos para concluir sua nova instalação ou atualização para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização pausa ou para, e uma mensagem explicativa aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

## Efeito da Licença de Direitos Híbridos na conexão do host

Existem três cenários em que a conexão do host com os hosts da nuvem pública é afetada com base no direito à Licença de Direitos Híbridos:

- Para criar uma nova conexão de host com os hosts da nuvem pública, você deve ter a Licença de Direitos Híbridos.
- Se você tiver a Licença de Direitos Híbridos, mas a licença tiver expirado, as conexões existentes com os hosts da nuvem pública serão marcadas como não autorizadas e entrarão no modo de manutenção. Quando as conexões de host existentes estão no modo de manutenção, você não pode fazer o seguinte:
  - Adicionar ou modificar conexões de host
  - Criar catálogo e atualizar imagem

- Executar ações de energia

- Quando as conexões de host não autorizadas mudam para autorizadas, as conexões de hospedagem existentes são reativadas.

## Introdução

Opcionalmente, você pode criar sua primeira conexão com os recursos de hospedagem ao criar um Site. Posteriormente, você pode alterar essa conexão e criar outras conexões. A configuração de uma conexão inclui a seleção do tipo de conexão entre os hipervisores suportados e o armazenamento e a rede que você seleciona dos recursos para essa conexão.

Administradores Somente Leitura podem visualizar detalhes de conexão e recursos. Você deve ser um Administrador Completo para executar tarefas de gerenciamento de conexão e recursos. Para obter detalhes, consulte Administração delegada.

### Onde encontrar informações sobre tipos de conexão

Você pode usar as plataformas de virtualização suportadas para hospedar e gerenciar máquinas em seu ambiente Citrix Virtual Apps ou Citrix Virtual Desktops. O artigo Requisitos do sistema lista os tipos suportados.

Para obter detalhes, consulte as seguintes fontes de informação:

- **XenServer (anteriormente Citrix Hypervisor™):**
  - Ambientes de virtualização XenServer.
  - Documentação do XenServer®.
- **Nutanix Acropolis:**
  - Ambientes de virtualização Nutanix.
  - Documentação do Nutanix.
- **VMware:**
  - Ambientes de virtualização VMware.
  - Documentação do produto VMware.
- **Microsoft Hyper-V:**
  - Ambientes de virtualização do Microsoft System Center Virtual Machine Manager (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/msscvmm.html).

    - Documentação da Microsoft.

- **Conexões de host de nuvem pública (AWS, Google Cloud, Microsoft Azure, soluções de nuvem e parceiros Nutanix e soluções de nuvem e parceiros VMware):** Para obter informações relacionadas a hosts de nuvem pública, consulte Configurar tipo de recurso.

> **Observação:**
>
> As fontes de informação direcionam você para a documentação do Citrix DaaS™. Se você estiver familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local apresenta várias diferenças. No Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio. As atualizações são lançadas para o serviço aproximadamente a cada quatro semanas. Assim, você pode descobrir que certos recursos disponíveis com o serviço não estão disponíveis na versão local.

## Armazenamento do host

Um produto de armazenamento é compatível quando gerenciado por um hipervisor compatível. O Citrix Support auxilia esses fornecedores de produtos de armazenamento na solução de problemas e na resolução de problemas, e documenta esses problemas no centro de conhecimento, conforme necessário.

Ao provisionar máquinas, os dados são classificados por tipo:

- Dados do sistema operacional (SO), que incluem imagens mestre.
- Dados temporários. Esses dados incluem todos os dados não persistentes gravados em máquinas provisionadas por MCS, arquivos de paginação do Windows, dados de perfil de usuário e quaisquer dados sincronizados com o ShareFile. Esses dados são descartados cada vez que uma máquina é reiniciada.

Fornecer armazenamento separado para cada tipo de dado pode reduzir a carga e melhorar o desempenho em cada dispositivo de armazenamento, aproveitando ao máximo os recursos disponíveis do host. Também permite que o armazenamento apropriado seja usado para os diferentes tipos de dados – persistência e resiliência são mais importantes para alguns dados do que para outros.

O armazenamento pode ser compartilhado (localizado centralmente, separado de qualquer host, usado por todos os hosts) ou local para um hipervisor. Por exemplo, o armazenamento compartilhado central pode ser um ou mais volumes de armazenamento clusterizados do

Windows Server 2012 (com ou sem armazenamento anexado), ou um appliance de um fornecedor de armazenamento. O armazenamento central também pode fornecer suas próprias otimizações, como caminhos de controle de armazenamento de hipervisor e acesso direto por meio de plug-ins de parceiros.

Armazenar dados temporários localmente evita ter que atravessar a rede para acessar o armazenamento compartilhado. Também reduz a carga no dispositivo de armazenamento compartilhado. O armazenamento compartilhado pode ser mais caro, então armazenar dados localmente pode reduzir despesas. Esses benefícios devem ser ponderados em relação à disponibilidade de armazenamento suficiente nos servidores do hipervisor.

Ao criar uma conexão, você escolhe um de dois métodos de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local para o hipervisor.

Ao usar armazenamento local em um ou mais hosts XenServer para armazenamento temporário de dados, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter®, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

### Armazenamento compartilhado por hipervisores

O método de armazenamento compartilhado por hipervisores armazena dados que precisam de persistência de longo prazo centralmente, fornecendo backup e gerenciamento centralizados. Esse armazenamento contém os discos do SO.

Ao selecionar este método, você pode escolher se deseja usar armazenamento local (em servidores no mesmo pool de hipervisores) para dados temporários da máquina. Este método não requer persistência ou tanta resiliência quanto os dados no armazenamento compartilhado, conhecido como *cache de dados temporários*. O disco local ajuda a reduzir o tráfego para o armazenamento principal do SO. Este disco é limpo após cada reinício da máquina. O disco é acessado por meio de um cache de memória write-through. Se você usar armazenamento local para dados temporários, o VDA provisionado estará vinculado a um host de hipervisor específico. Se esse host falhar, a VM não poderá iniciar.

**Exceção**: O Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários em armazenamento local ao usar Volumes de Armazenamento em Cluster (CSV).

Crie uma conexão para armazenar dados temporários localmente e, em seguida, habilite e configure valores não padrão para o tamanho do disco de cache e o tamanho da memória de cada

VM. Os valores padrão são adaptados ao tipo de conexão e são suficientes para a maioria dos casos. Para obter detalhes, consulte Criar catálogos de máquinas.

O hipervisor também pode fornecer tecnologias de otimização por meio do cache de leitura das imagens de disco localmente. Por exemplo, o XenServer oferece o IntelliCache™, que reduz o tráfego de rede para o armazenamento central.

### Armazenamento local ao hipervisor

O método de armazenamento local ao hipervisor armazena dados localmente no hipervisor. Com esse método, as imagens mestre e outros dados do SO são transferidos para os hipervisores no Site. Esse processo ocorre para a criação inicial da máquina e futuras atualizações de imagem. Esse processo resulta em tráfego significativo na rede de gerenciamento. As transferências de imagem também consomem muito tempo, e as imagens ficam disponíveis para cada host em um momento diferente.

## Criar uma conexão e recursos

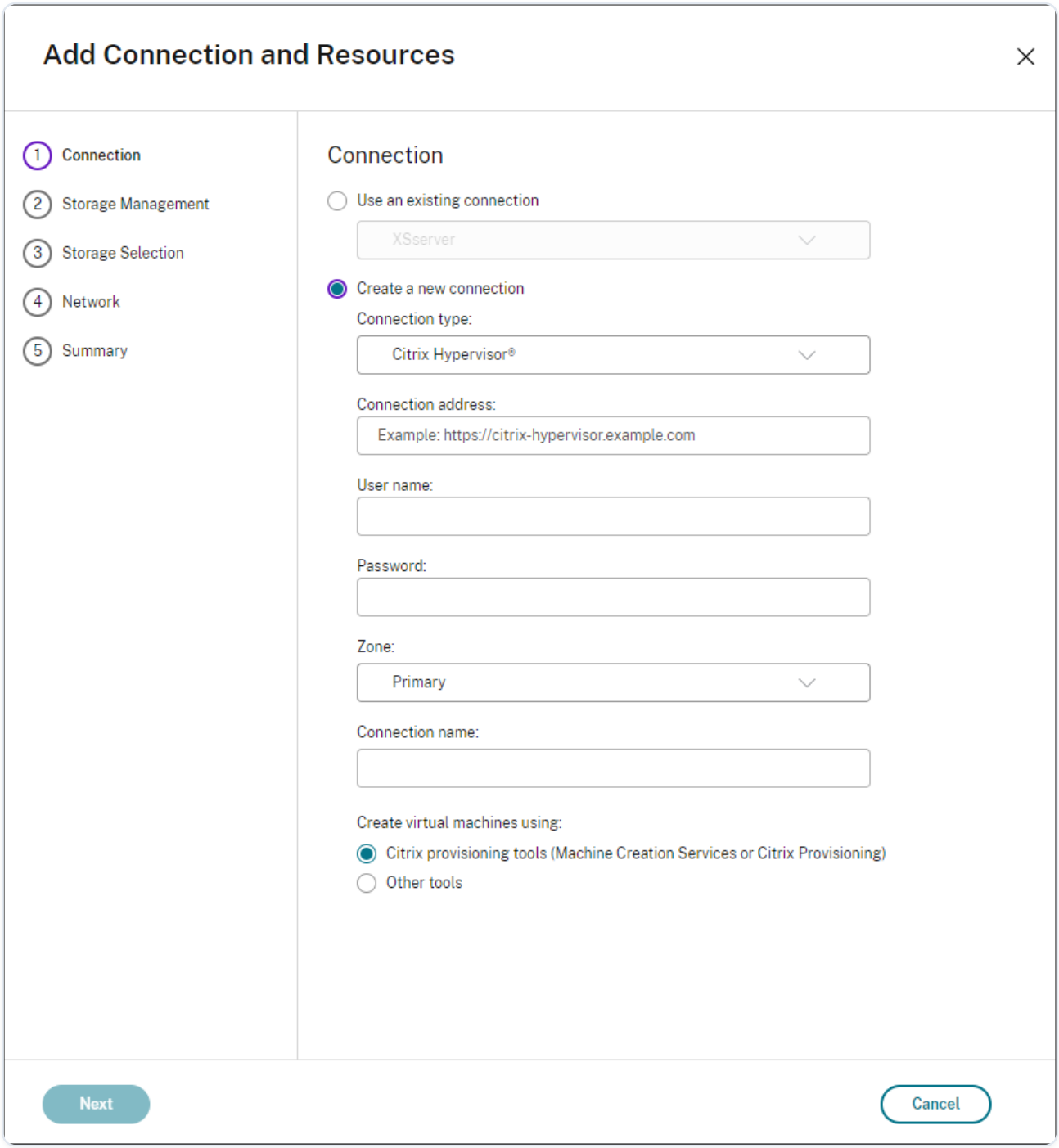
Opcionalmente, você pode criar a primeira conexão ao criar o Site. O assistente de criação do Site contém as páginas relacionadas à conexão descritas nas seções a seguir.

Se você estiver criando uma conexão depois de criar o Site, comece com a etapa 1.

> **Importante:**
>
> Os recursos do host (armazenamento e rede) devem estar disponíveis antes de você criar uma conexão.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione **Adicionar Conexões e Recursos** na barra de ações.
4. O assistente o guiará pelas seguintes páginas (o conteúdo específico da página depende do tipo de conexão selecionado). Após concluir cada página, clique em **Avançar** até chegar à página **Resumo**.

### Conexão




Na página **Conexão**:

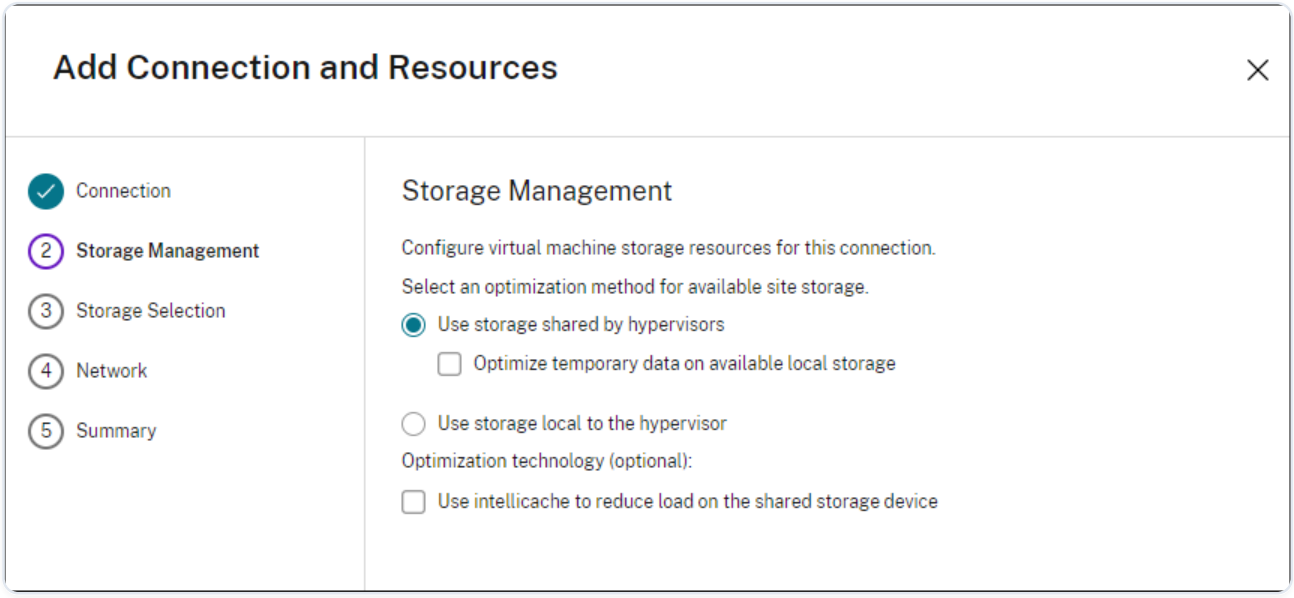
- Para criar uma conexão, selecione **Criar uma nova Conexão**. Para criar uma conexão com base na mesma configuração de host de uma conexão existente, selecione **Usar uma Conexão existente** e, em seguida, escolha a conexão relevante.
- Selecione o hipervisor que você está usando no campo **Tipo de conexão**. As conexões de host de nuvem pública são listadas na lista suspensa somente se você usar a Licença de Direitos Híbridos. Alternativamente, você pode usar o comando PowerShell `Get-`

`HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true para obter o seguinte:

  - Lista de todos os plug-ins de hipervisor compatíveis com Citrix, incluindo plug-ins de terceiros.
  - Disponibilidade do plug-in do hipervisor. Se o status de disponibilidade for **false**, o motivo possível pode ser que o plug-in do hipervisor não esteja instalado corretamente ou você não tenha direito à Licença de Direitos Híbridos.

- Os campos de endereço de conexão e credenciais diferem, dependendo do tipo de conexão selecionado. Insira as informações solicitadas.
- Insira um nome de conexão. Este nome aparece no Web Studio.
- Escolha a ferramenta que você usa para criar máquinas virtuais: ferramentas do Web Studio (como Machine Creation Services™ ou Citrix Provisioning) ou outras ferramentas.

## Gerenciamento de armazenamento




Para obter informações sobre tipos e métodos de gerenciamento de armazenamento, consulte Armazenamento do host.

Se você estiver configurando uma conexão com um host Hyper-V ou VMware, navegue até e selecione um nome de cluster. Outros tipos de conexão não solicitam um nome de cluster.

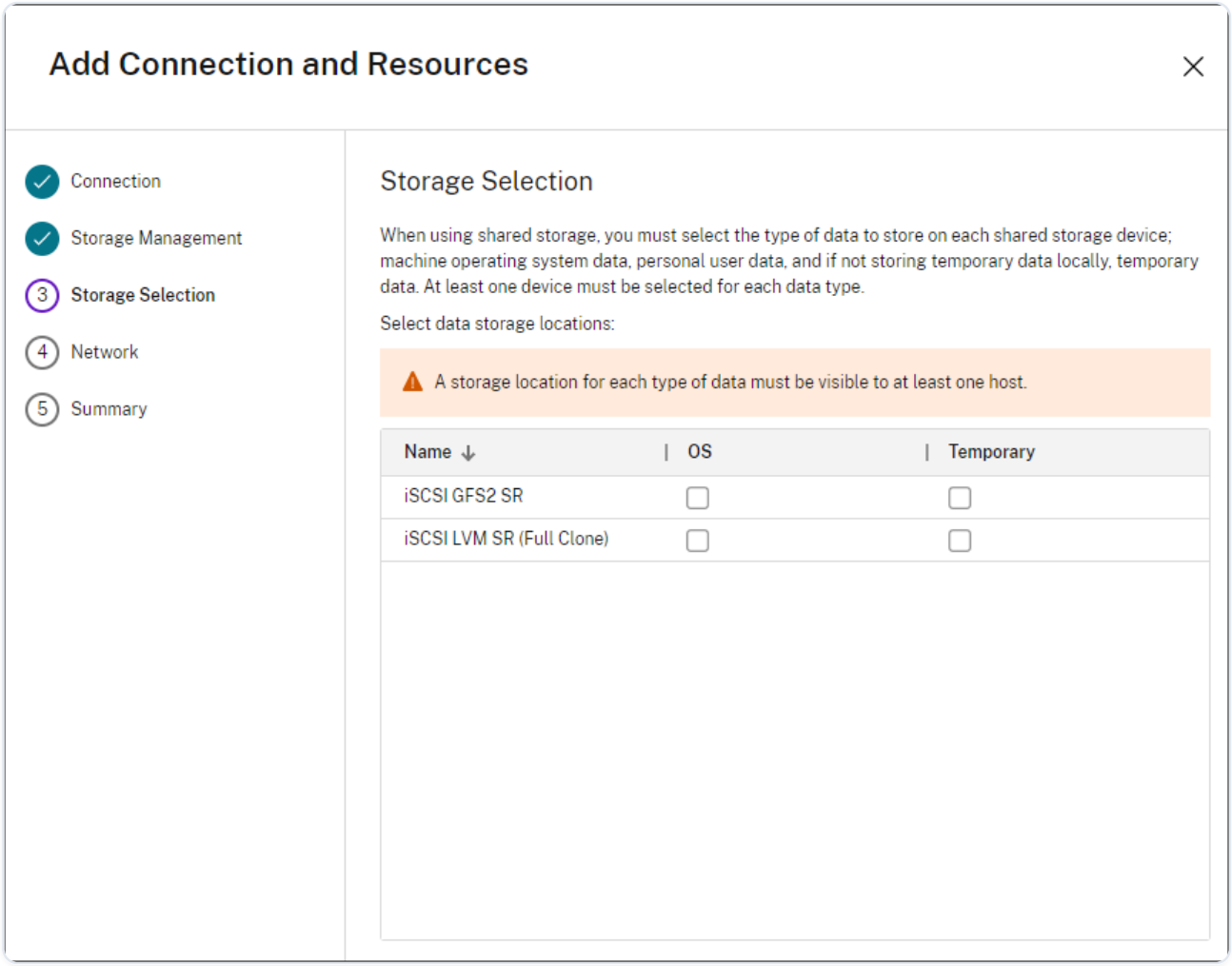
Selecione um método de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local ao hipervisor.

- Se você escolher armazenamento compartilhado por hipervisores, indique se deseja manter dados temporários no armazenamento local disponível. (Você pode especificar tamanhos de

armazenamento temporário não padrão nos catálogos de máquinas que usam esta conexão.)
**Exceção:** Ao usar Volumes de Armazenamento Clusterizados (CSV), o Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários no armazenamento local. A configuração desse gerenciamento de armazenamento no Web Studio falha.

Se você usar armazenamento compartilhado em um pool XenServer, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Usar IntelliCache para conexões XenServer.

### Seleção de armazenamento




Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento do host.

Selecione pelo menos um dispositivo de armazenamento de host para cada tipo de dados disponível. O método de gerenciamento de armazenamento selecionado na página anterior afeta quais tipos de dados estão disponíveis para seleção nesta página. Selecione pelo menos um

dispositivo de armazenamento para cada tipo de dados suportado antes de prosseguir para a próxima página do assistente.

A parte inferior da página **Seleção de Armazenamento** contém mais opções de configuração se você escolheu armazenamento compartilhado por hipervisores e ativou **Otimizar dados temporários no armazenamento local disponível** na página anterior. Você pode selecionar quais dispositivos de armazenamento local usar para dados temporários.

O número de dispositivos de armazenamento atualmente selecionados é mostrado (no gráfico anterior, "1 dispositivo de armazenamento selecionado"). Ao passar o mouse sobre essa entrada, os nomes dos dispositivos selecionados aparecem.

1. Clique em **Selecionar** para alterar os dispositivos de armazenamento a serem usados.
2. Na caixa de diálogo **Selecionar Armazenamento**, marque ou desmarque as caixas de seleção do dispositivo de armazenamento e, em seguida, clique em **OK**.

### Rede

Na página **Rede**, insira um nome para os recursos. Este nome aparece no Web Studio para identificar a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs usam.

### Resumo

Na página **Resumo**, revise suas seleções. Quando terminar, clique em **Concluir**.

**Lembre-se**: Armazenar dados temporários localmente permite configurar valores não padrão para o armazenamento de dados temporários ao criar o Catálogo de Máquinas que contém máquinas usando esta conexão. Consulte Criar Catálogos de Máquinas.

## Editar configurações de conexão

Não use este procedimento para renomear uma conexão ou para criar uma conexão. Essas são operações diferentes. Altere o endereço somente se a máquina host atual tiver um novo endereço. Inserir um endereço para uma máquina diferente quebrará os Catálogos de Máquinas da conexão.

Você não pode alterar as configurações de **GPU** para uma conexão, porque os Catálogos de Máquinas que acessam este recurso devem usar uma imagem mestre apropriada e específica para GPU. Crie uma conexão.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.

3. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
4. Siga as orientações para as configurações disponíveis ao editar uma conexão.
5. Quando terminar, clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Página **Propriedades da Conexão**:

- Para alterar o endereço e as credenciais da conexão, selecione **Editar configurações...** e insira as novas informações.
- Para especificar os servidores de alta disponibilidade para uma conexão XenServer, selecione **Editar servidores...** e selecione os servidores. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o XenServer caso o mestre do pool falhe.

> **Observação:**
>
> Se você estiver usando HTTPS e quiser configurar servidores de alta disponibilidade, não instale um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor.

Página **Avançado**:

- Para um tipo de conexão Wake on LAN do Microsoft System Center Configuration Manager (ConfMgr), que é usado com o Acesso Remoto ao PC, insira **ConfMgr Wake Proxy**, pacotes mágicos e informações de transmissão de pacotes.
- As configurações de limite de aceleração permitem especificar um número máximo de ações de energia permitidas em uma conexão. Essas configurações podem ajudar quando as configurações de gerenciamento de energia permitem que muitas ou poucas máquinas iniciem ao mesmo tempo. Cada tipo de conexão tem valores padrão específicos que são apropriados para a maioria dos casos e não devem ser alterados.
- A configuração **Ações simultâneas (todos os tipos)** especifica dois valores: um número absoluto máximo que pode ocorrer simultaneamente nesta conexão e uma porcentagem máxima de todas as máquinas que usam esta conexão. Você deve especificar valores absolutos e percentuais. O limite real aplicado é o menor dos valores.

  Por exemplo, em uma implantação com 34 máquinas, se **Ações simultâneas (todos os tipos)** for definido como um valor absoluto de 10 e um valor percentual de 10, o limite real

aplicado é 3 (ou seja, 10% de 34 arredondado para o número inteiro mais próximo, que é menor que o valor absoluto de 10 máquinas).

- O **Número máximo de novas ações por minuto** é um número absoluto. Não há valor percentual.
- Insira informações no campo **Opções de conexão** somente sob a orientação de um representante do Suporte Citrix ou instruções explícitas da documentação.

Página **Locatários Compartilhados**:

Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura desta conexão. Como resultado, ao criar ou atualizar catálogos, você pode selecionar imagens compartilhadas desses locatários e assinaturas.

- Insira o **ID do Aplicativo** e o **Segredo do Aplicativo** para o aplicativo associado a esta conexão. Com essas informações, você pode autenticar no Azure. Recomendamos que você altere as chaves regularmente para garantir a segurança.
- Especifique locatários e assinaturas compartilhados. Você pode adicionar até oito locatários compartilhados. Para cada locatário, você pode adicionar até oito assinaturas.
- Clique em **Salvar** e **Aplicar** quando terminar.

Insira informações no campo **Opções de conexão** somente sob a orientação de um representante do Suporte Citrix.

## Editar redes

Você pode alterar as redes para uma conexão. Faça o seguinte:

1. Vá para **Hospedagem**.
2. Selecione os recursos de destino na conexão e, em seguida, selecione **Editar Rede** na barra de ações.
3. Selecione uma ou mais redes para as máquinas virtuais usarem.
4. Clique em **Salvar** para salvar suas alterações e sair.

## Ativar ou desativar o modo de manutenção para uma conexão

Ativar o modo de manutenção para uma conexão impede que qualquer nova ação de energia afete qualquer máquina armazenada na conexão. Os usuários não podem se conectar a uma máquina quando ela está no modo de manutenção. Se os usuários já estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão. Para ativar o modo de manutenção, selecione **Ativar Modo de Manutenção** na barra de ações. Para desativar o modo de manutenção, selecione **Desativar Modo de Manutenção**.

Você também pode ativar ou desativar o modo de manutenção para máquinas individuais. Além disso, você pode ativar ou desativar o modo de manutenção para máquinas em Catálogos de Máquinas ou Grupos de Entrega.

## Excluir uma conexão

A exclusão de uma conexão pode resultar na exclusão de um grande número de máquinas e na perda de dados. Certifique-se de que os dados do usuário nas máquinas afetadas estejam com backup ou não sejam mais necessários.

Antes de excluir uma conexão, certifique-se de que:

- Todos os usuários fizeram logoff das máquinas armazenadas na conexão.
- Nenhuma sessão de usuário desconectada está em execução.
- O modo de manutenção está ativado para máquinas agrupadas e dedicadas.
- Todas as máquinas nos Catálogos de Máquinas usados pela conexão são desligadas.

Um Catálogo de Máquinas torna-se inutilizável quando você exclui uma conexão que é referenciada por esse catálogo. Se esta conexão for referenciada por um catálogo, você tem a opção de excluir o catálogo. Antes de excluir um catálogo, certifique-se de que ele não seja usado por outras conexões.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e então selecione **Excluir Conexão** na barra de ações.
4. Se esta conexão tiver máquinas armazenadas nela, será perguntado se as máquinas devem ser excluídas. Se elas forem excluídas, especifique o que deve ser feito com as contas de computador do Active Directory associadas.

## Renomear ou testar uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.

3. Selecione a conexão e, em seguida, selecione **Renomear Conexão** ou **Testar Conexão** na barra de ações.

## Exibir detalhes da máquina em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Exibir Máquinas** na barra de ações.

O painel superior lista as máquinas acessadas pela conexão. Selecione uma máquina para ver seus detalhes no painel inferior. Os detalhes da sessão também são fornecidos para sessões abertas.

Use o recurso de pesquisa para encontrar máquinas rapidamente. Selecione uma pesquisa salva na lista na parte superior da janela ou crie uma pesquisa. Você pode pesquisar digitando todo ou parte do nome da máquina, ou pode construir uma expressão para usar em uma pesquisa avançada. Para construir uma expressão, clique em **Desdobrar** e, em seguida, selecione nas listas de propriedades e operadores.

## Gerenciar máquinas em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione uma conexão e, em seguida, selecione **Exibir Máquinas** no painel **Ação**.
4. Selecione uma das seguintes opções na barra de ações. Algumas ações não estão disponíveis, dependendo do estado da máquina e do tipo de host da conexão.

| AÇÃO | DESCRIÇÃO |
|---|---|
| Iniciar | Inicia a máquina se ela estiver desligada ou suspensa. |
| Suspender | Pausa a máquina sem desligá-la e atualiza a lista de máquinas. |
| Desligar | Solicita ao sistema operacional que desligue. |
| Forçar desligamento | Desliga a máquina à força e atualiza a lista de máquinas. |

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| Reiniciar | Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, o desktop permanecerá em seu estado atual. |
| Ativar modo de manutenção | Interrompe temporariamente as conexões com uma máquina. Os usuários não podem se conectar a uma máquina neste estado. Se os usuários estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff. (Você também pode ativar ou desativar o modo de manutenção para todas as máquinas acessadas por meio de uma conexão, conforme descrito acima.) |
| Remover do Grupo de Entrega | Remover uma máquina de um Grupo de Entrega não a exclui do Catálogo de Máquinas que o Grupo de Entrega usa. Você só pode remover uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver removendo a máquina. |
| Excluir | Quando você exclui uma máquina, os usuários não têm mais acesso a ela, e a máquina é excluída do Catálogo de Máquinas. Antes de excluir uma máquina, certifique-se de que todos os dados do usuário estejam com backup ou não sejam mais necessários. Você só pode excluir uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver excluindo a máquina. |

Para ações que envolvem o desligamento da máquina, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

## Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar dados temporários e do sistema operacional para VMs que usam uma conexão. Você também pode especificar quais servidores usar para o armazenamento de cada tipo de dado.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Editar Armazenamento** na barra de ações.
4. No painel esquerdo, selecione o tipo de dados: sistema operacional ou temporário.
5. Marque ou desmarque as caixas de seleção para um ou mais dispositivos de armazenamento para o tipo de dados selecionado.
6. Clique em **OK**.

Cada dispositivo de armazenamento na lista inclui seu nome e status de armazenamento. Os valores de status de armazenamento válidos são:

- **Em uso:** O armazenamento está sendo usado para criar máquinas.
- **Substituído:** O armazenamento está sendo usado apenas para máquinas existentes. Nenhuma máquina nova é adicionada a este armazenamento.
- **Não em uso:** O armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo que está atualmente **Em uso**, seu status muda para **Substituído**. As máquinas existentes continuarão a usar esse dispositivo de armazenamento (e podem gravar dados nele), portanto, é possível que esse local fique cheio mesmo depois de parar de ser usado para criar máquinas.

## Excluir, renomear ou testar recursos

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione o recurso e, em seguida, selecione a entrada apropriada na barra de ações: **Excluir Recursos**, **Renomear Recursos** ou **Testar Recursos**.

## Detectar recursos órfãos do Azure

Recursos órfãos são recursos não utilizados presentes no sistema e podem levar a despesas desnecessárias.

Este recurso permite detectar os recursos órfãos do Azure nos hosts do seu site Citrix Virtual Apps and Desktops.

Siga as etapas no Web Studio:

1. Em **Gerenciar**, selecione **Hospedagem** no painel esquerdo.
2. Selecione uma conexão e, em seguida, selecione **Detectar Recursos Órfãos** na barra de ações. A caixa de diálogo **Detectar Recursos Órfãos** exibe o relatório de recursos órfãos.
3. Para visualizar o relatório de recursos órfãos, selecione **Visualizar Relatório**.

Alternativamente, você pode detectar recursos órfãos do Azure usando o PowerShell. Para obter mais informações, consulte Recuperar uma lista de recursos órfãos.

Para entender as razões por trás dos recursos órfãos e aprender como prosseguir, consulte Gerenciar recursos órfãos do Azure de forma eficiente com o Citrix.

## Temporizadores de conexão

Você pode usar as configurações de política para configurar três temporizadores de conexão:

- **Temporizador máximo de conexão:** Determina a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop virtual. Use as configurações de política **Temporizador de conexão de sessão** e **Intervalo do temporizador de conexão de sessão**.
- **Temporizador de inatividade da conexão:** Determina por quanto tempo uma conexão ininterrupta de dispositivo de usuário com um desktop virtual é mantida se não houver entrada do usuário. Use as configurações de política **Temporizador de inatividade da sessão** e **Intervalo do temporizador de inatividade da sessão**.
- **Temporizador de desconexão:** Determina por quanto tempo um desktop virtual desconectado e bloqueado pode permanecer bloqueado antes que a sessão seja encerrada. Use as configurações de política **Temporizador de sessão desconectada** e **Intervalo do temporizador de sessão desconectada**.

Ao atualizar qualquer uma dessas configurações, certifique-se de que elas sejam consistentes em toda a sua implantação.

Consulte a documentação de configurações de política para obter mais informações.

## Recuperar uma lista de recursos órfãos

Você pode obter uma lista de recursos órfãos que são criados pelo MCS, mas não são mais rastreados pelo MCS. Isso é atualmente aplicável a ambientes Azure. Para obter a lista, você pode usar comandos PowerShell. Você pode filtrar usando conexões.

**Nota:**

- O comando PowerShell é rejeitado se qualquer provisionamento ou atualização de imagem estiver em andamento.
- Um recurso gerenciado pelo cliente marcado com todas as tags Citrix é detectado como um recurso órfão. No entanto, se você adicionar outra tag CitrixDetectIgnore com o valor true a esse recurso, o recurso será ignorado durante a detecção de recursos órfãos.

### Limitações

- Somente um usuário administrador com função de administrador completo integrado ou administrador de nuvem pode executar o comando PowerShell e obter a lista de recursos órfãos.
- Para evitar o reconhecimento incorreto de recursos órfãos, não ligue as VMs enquanto estiver filtrando recursos órfãos.
- Cerca de 2.000 registros são exibidos como órfãos em caso de possível carga de trabalho pesada.

Para exibir a lista de recursos órfãos:

1. Abra uma janela do **PowerShell**.
2. Execute os seguintes comandos:
   a. Obtenha o UID da conexão. O UID da conexão é o valor do atributo HypervisorConnectionUid.

      ```
      Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
      'Azure*' }"
      ```

   b. Obtenha a lista de recursos órfãos.

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

Para exibir a lista de recursos órfãos a partir de um ID de assinatura:

1. Abra uma janela do **PowerShell**.
2. Execute os seguintes comandos:
   a. Encontre o UID da conexão usando o ID da assinatura. O UID da conexão é o valor do atributo HypervisorConnectionUid.

```
Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
-match '<subscriptionId>' }
```

   b. Obtenha a lista de recursos órfãos:

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

**Observação:**

Verifique os recursos cuidadosamente antes de excluí-los.

## Onde ir em seguida

Para obter informações sobre conexão com tipos de host específicos, consulte:

- Conexão com AWS
- Conexão com XenServer
- Conexão com ambientes de nuvem do Google
- Conexão com Microsoft Azure
- Conexão com Microsoft System Center Virtual Machine Manager
- Conexão com Nutanix
- Conexão com soluções de nuvem e parceiros Nutanix
- Conexão com VMware
- Conexão com soluções de nuvem e parceiros VMware

Se você estiver no processo de implantação inicial, crie um catálogo de máquinas.

## Conexão com AWS

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem AWS.

> **Observação:**
>
> Antes de criar uma conexão com a AWS, você precisa primeiro concluir a configuração da sua conta AWS como um local de recurso. Consulte Ambientes de nuvem AWS.

### Criar uma conexão

Ao criar uma conexão a partir do Web Studio:

- Você deve fornecer os valores da chave de API e da chave secreta. Você pode exportar o arquivo de chave contendo esses valores da AWS e depois importá-los. Você também deve fornecer a região, zona de disponibilidade, nome da VPC, endereços de sub-rede, nome de domínio, nomes de grupos de segurança e credenciais.
- O arquivo de credenciais para a conta raiz da AWS (recuperado do console da AWS) não é formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão da AWS. Portanto, o gerenciamento do Citrix Virtual Apps and Desktops™ não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Certifique-se de que você está usando arquivos de credenciais do AWS Identity Access Management (IAM).

> **Observação:**
>
> Depois de criar uma conexão, as tentativas de atualizar a chave de API e a chave secreta podem falhar. Para resolver o problema, verifique as restrições do seu servidor proxy ou firewall e certifique-se de que o seguinte endereço possa ser contatado: `https://*.amazonaws.com`.

#### Valores padrão da conexão do host

Ao criar conexões de host em ambientes de nuvem AWS, os seguintes valores padrão são exibidos:

| OPÇÃO | ABSOLUTO | PORCENTAGEM |
|---|---|---|
| Ações simultâneas (todos os tipos) | 125 | 100 |
| Máximo de novas ações por minuto | 125 | |

O MCS suporta 100 operações de provisionamento simultâneas máximas por padrão.

## URL do endpoint de serviço

### URL do endpoint de serviço da zona padrão

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

## Definir permissões do IAM

Use as informações nesta seção para definir permissões IAM para Citrix Virtual Apps and Desktops na AWS. O serviço IAM da Amazon permite contas com vários usuários, que podem ser ainda mais organizados em grupos. Esses usuários podem possuir diferentes permissões para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões IAM, consulte referência de política JSON do IAM.

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

1. Faça login no console de gerenciamento da AWS e selecione o **serviço IAM** na lista suspensa.
2. Selecione **Criar um Novo Grupo de Usuários**.
3. Digite um nome para o novo grupo de usuários e selecione **Continuar**.
4. Na página **Permissões**, escolha **Política Personalizada**. Selecione **Selecionar**.
5. Digite um nome para a **política de Permissões**.
6. Na seção **Documento de Política**, insira as permissões relevantes.

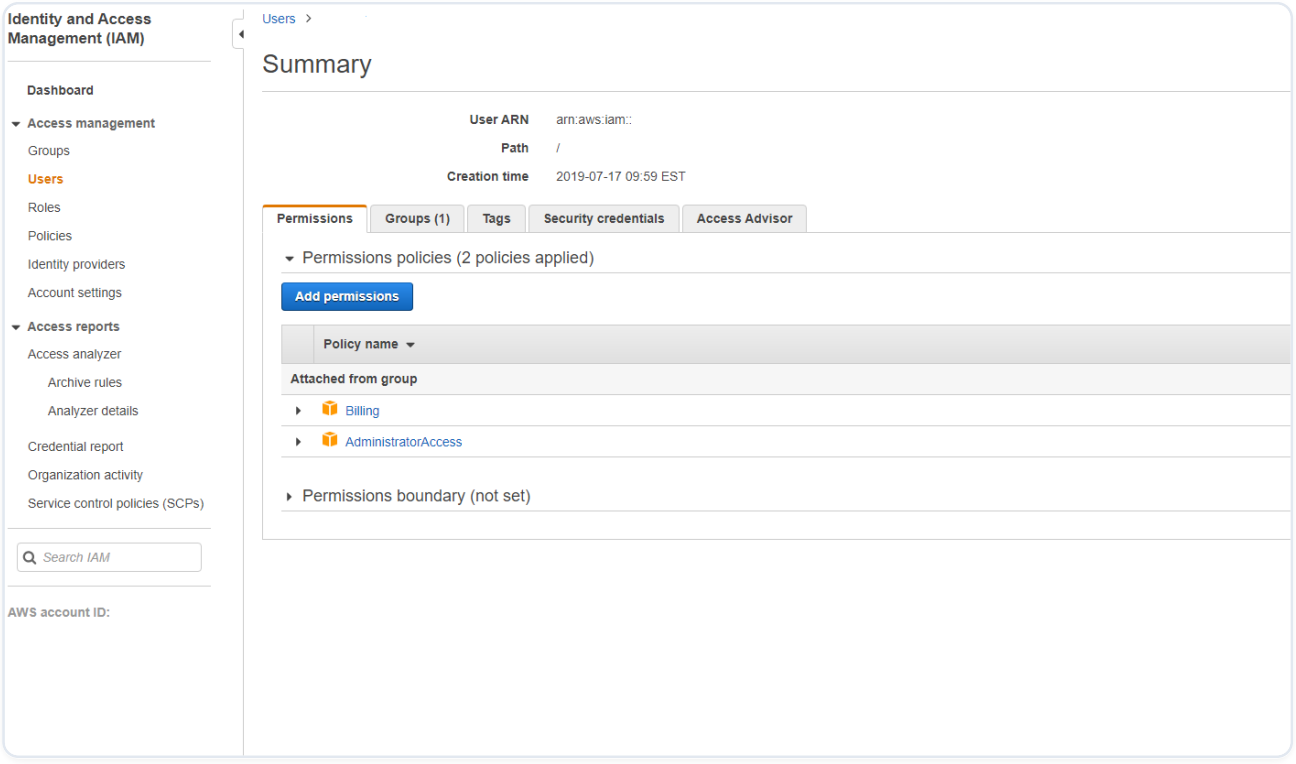
Após inserir as informações da política, selecione **Continuar** para concluir o grupo de usuários. Os usuários do grupo recebem permissões para realizar apenas as ações necessárias para o Citrix Virtual Apps and Desktops.

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

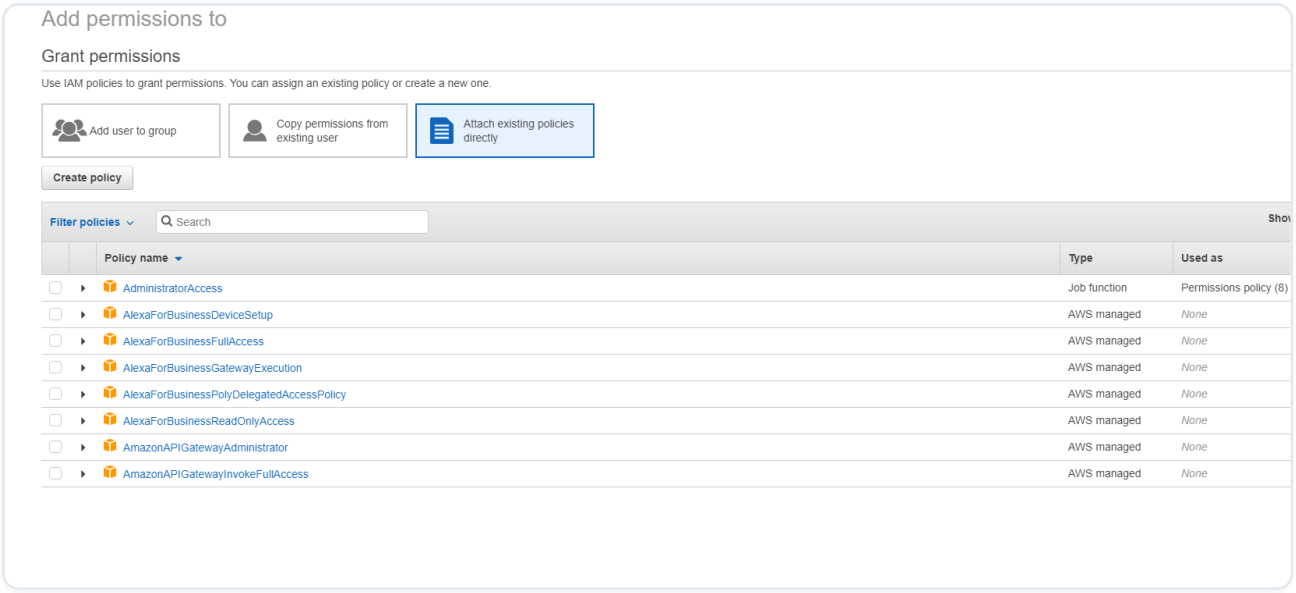
### Definir permissões IAM

Defina as permissões na seção **IAM** do Console de Gerenciamento da AWS:

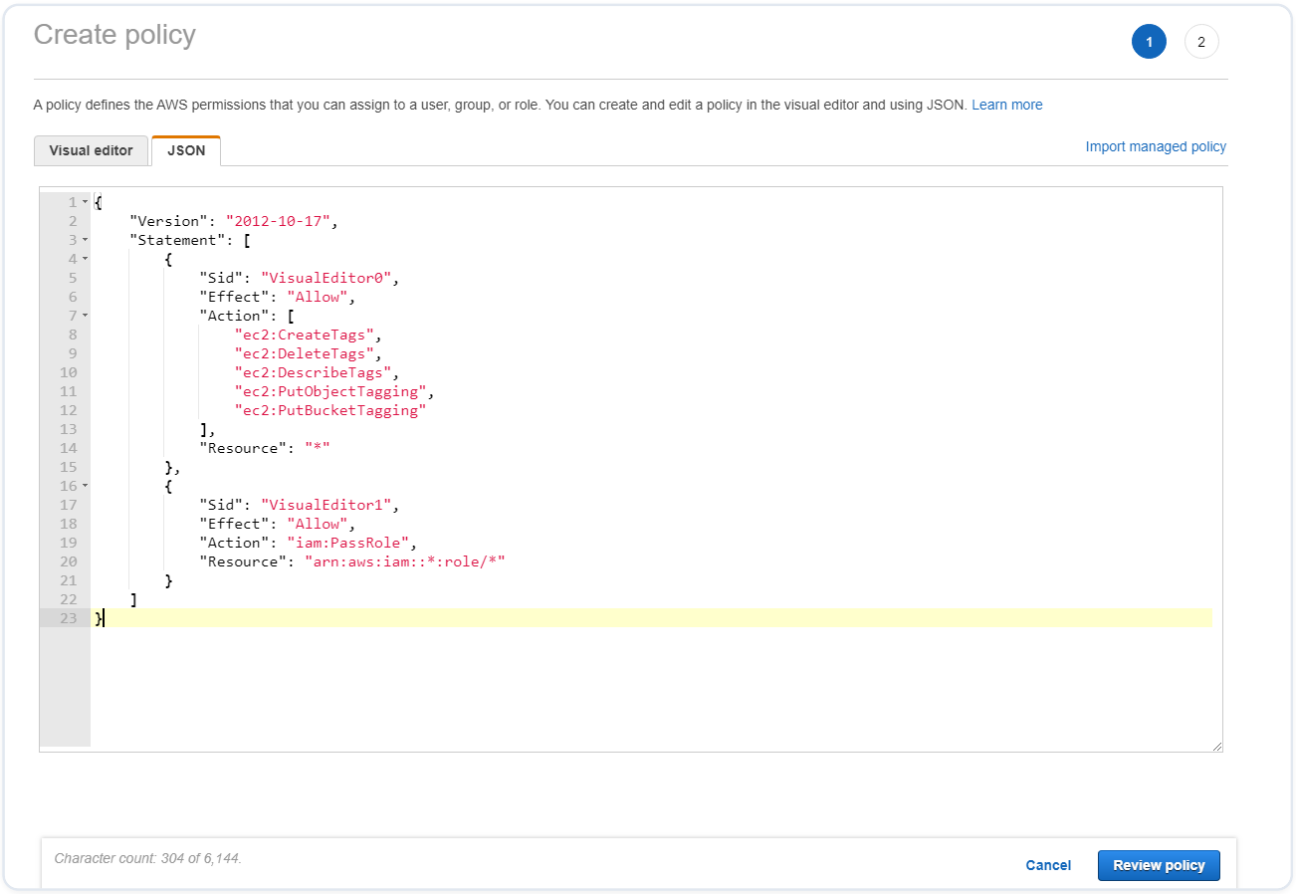
1. No painel **Resumo**, selecione a guia **Permissões**.
2. Selecione **Adicionar permissões.**




Na tela **Adicionar Permissões a**, conceda permissões:




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




**Dica:**

O exemplo JSON mencionado pode não incluir todas as permissões para seu ambiente. Consulte Como Definir Permissões de Gerenciamento de Acesso de Identidade Executando Citrix Virtual Apps and Desktops no AWS para obter mais informações.

## Permissões AWS necessárias

Esta seção contém a lista completa de permissões do AWS.

> **Observação:**
>
> A permissão *iam:PassRole* é necessária apenas para **role_based_auth**.

### Criando uma conexão de host

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

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSubnets",

                "ec2:DescribeVpcs",

                "ec2:DescribeRegions",

                "ec2:DescribeSnapshots",

                "ec2:DescribeLaunchTemplates"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

### Gerenciamento de energia de VMs

As instâncias de máquina são ligadas ou desligadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances",
```

```
                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

### Criar, atualizar ou excluir VMs

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

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",
```

```
                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus"

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
```

```
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
```

```
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

> **Observação:**
>
> A seção EC2 relacionada a grupos de segurança é necessária apenas se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.

### UPLOAD E DOWNLOAD DIRETO DE DISCO

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

> **Observação:**
>
> O suporte para volume worker foi descontinuado.

> As seguintes permissões devem ser adicionadas à política:

- `ebs:StartSnapshot`

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

**Importante:**

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

### Criptografia EBS de volumes criados

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

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",
```

```
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

**Observação:**

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

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
```

```
                "kms:DescribeKey",

                "kms:GenerateDataKeyWithoutPlainText",

                "kms:ReEncryptTo",

                "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

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

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",
```

```
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

Para obter mais informações, consulte documentação oficial do AWS Key Management Service.

### Autenticação baseada em função do IAM

As seguintes permissões são adicionadas para suportar a autenticação baseada em função.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

### Política de permissões mínimas do IAM

O JSON a seguir pode ser usado para todos os recursos atualmente suportados. Você pode criar conexões de host, criar, atualizar ou excluir VMs e fazer gerenciamento de energia usando esta

política. A política pode ser aplicada aos usuários conforme explicado nas seções Definir permissões IAM ou você também pode usar autenticação baseada em função usando a chave de segurança e a chave secreta **role_based_auth**.

**Importante:**

Para usar **role_based_auth**, primeiro configure a função IAM desejada em todos os Delivery Controllers em nosso site. Usando o Web Studio, adicione a conexão de hospedagem e forneça o role_based_auth para a chave de autenticação e o segredo. Uma conexão de hospedagem com essas configurações usa então a autenticação baseada em função.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",
```

```
                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",
```

```
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
```

```
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
```

```
            "Resource": "*"

        },

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

**Observação:**

- A seção EC2 relacionada a SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são necessárias.
- A seção KMS é necessária apenas ao usar a criptografia de volume EBS.
- A seção de permissão iam:PassRole é necessária apenas para **role_based_auth**.
- Permissões específicas em nível de recurso podem ser adicionadas em vez de acesso total, com base em seus requisitos e ambiente. Consulte os documentos da AWS Desmistificando as Permissões em Nível de Recurso do EC2 e Gerenciamento de acesso para recursos da AWS para obter mais detalhes.

## Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do AWS, consulte Criar um catálogo AWS

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com XenServer®

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de virtualização XenServer.

> **Observação:**
>
> Antes de criar uma conexão com o XenServer, você precisa primeiro concluir a configuração da sua conta XenServer como um local de recurso. Consulte Ambientes de virtualização XenServer.

### Criar uma conexão com o XenServer

Ao criar uma conexão com o XenServer (anteriormente Citrix Hypervisor™), você deve fornecer as credenciais para um usuário com nível de VM Power Admin ou superior.

A Citrix recomenda usar HTTPS para proteger as comunicações com o XenServer. Para usar HTTPS, você deve substituir o certificado SSL padrão instalado no XenServer.

Você pode configurar a alta disponibilidade se ela estiver habilitada no servidor XenServer. Para versões do Citrix Virtual Apps and Desktops anteriores a 2507 LTSR, você não pode instalar um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor.

Você pode selecionar um tipo e grupo de GPU, ou pass-through, se o XenServer suportar vGPU. A exibição indica se a seleção possui recursos de GPU dedicados.

Ao usar armazenamento local em um ou mais hosts XenServer para armazenamento temporário de dados, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter®, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

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

- BIOS herdado para VMs de SO de Desktop ou Servidor suportadas.

- UEFI para VMs de SO de Desktop ou Servidor suportadas, incluindo Secure Boot.

> **Nota:**
>
> São necessárias permissões de operador de pool ou superiores ao configurar o MCS.

#### Usar IntelliCache™ para conexões XenServer

Usando o IntelliCache, as implantações de VDI hospedadas são mais econômicas porque você pode usar uma combinação de armazenamento compartilhado e armazenamento local. Isso melhora o desempenho e reduz o tráfego de rede. O armazenamento local armazena em cache a imagem mestre do armazenamento compartilhado, o que reduz o número de leituras no armazenamento compartilhado. Para desktops compartilhados, as gravações nos discos de diferenciação são gravadas no armazenamento local no host e não no armazenamento compartilhado.

- O armazenamento compartilhado deve ser NFS ao usar o IntelliCache.
- A Citrix recomenda que você use um dispositivo de armazenamento local de alto desempenho para garantir a transferência de dados mais rápida possível.

Para usar o IntelliCache, você deve habilitá-lo neste produto e no XenServer.

- Ao instalar o XenServer, selecione **Habilitar provisionamento dinâmico (Armazenamento otimizado para Desktops Virtuais)**. A Citrix não oferece suporte a pools mistos de servidores que têm o IntelliCache habilitado e servidores que não o têm. Para obter mais informações, consulte a documentação do XenServer.
- No Citrix Virtual Apps and Desktops™, o IntelliCache é desabilitado por padrão. Você pode alterar a configuração apenas ao criar uma conexão XenServer; você não pode desabilitar o IntelliCache posteriormente. Ao adicionar uma conexão XenServer:
  - Selecione **Compartilhado** como o tipo de armazenamento.
  - Selecione a caixa de seleção **Usar IntelliCache**.

### Permissões necessárias do XenServer

As permissões do XenServer são baseadas em função (RBAC). O recurso Controle de Acesso Baseado em Função (RBAC) no XenServer permite atribuir usuários, funções e permissões para controlar quem tem acesso ao seu XenServer e quais ações eles podem executar. O sistema RBAC do XenServer mapeia um usuário (ou um grupo de usuários) para funções definidas (um

conjunto nomeado de permissões). As funções têm permissões XenServer associadas para executar certas operações.

Para obter mais informações, consulte Controle de acesso baseado em função.

A hierarquia de funções, em ordem crescente de permissões, é: Somente Leitura → Operador de VM → Administrador de VM → Administrador de Energia de VM → Operador de Pool → Administrador de Pool.

A seção a seguir resume a função mínima necessária para cada tarefa de provisionamento.

### Criando uma conexão de host

| TAREFA | FUNÇÃO MÍNIMA NECESSÁRIA |
|---|---|
| Adicionar uma conexão de host usando as informações obtidas do XenServer | Somente leitura |
| Visualizar usuários e suas funções atribuídas | Somente leitura |

### Gerenciamento de energia de VMs

| TAREFA | FUNÇÃO MÍNIMA NECESSÁRIA |
|---|---|
| Ligar ou desligar as VMs | Operador de VM |

### Criar, atualizar ou excluir VMs

| TAREFA | FUNÇÃO MÍNIMA NECESSÁRIA |
|---|---|
| Adicionar ou remover VMs de agendamentos de snapshots existentes | Administrador de energia de VM |
| Adicionar, modificar, excluir agendamentos de snapshots | Operador de Pool |
| Publicar imagem mestre | Operador de Pool (Requer bloqueio de porta de switch) |
| Criar um catálogo de máquinas | Operador de Pool: Requer bloqueio de porta de switch |
| Adicionar ou remover VMs (VMs não habilitadas para GPU) | Administrador de VM |

| TAREFA | FUNÇÃO MÍNIMA NECESSÁRIA |
| --- | --- |
| Adicionar ou remover VMs (VMs habilitadas para GPU) | Operador de Pool |
| Adicionar, remover ou configurar disco virtual ou dispositivos de CD | Administrador de VM |
| Gerenciar Tags | Operador de VM |

Para obter mais informações sobre funções e permissões RBAC, consulte funções e permissões RBAC.

Para obter informações sobre o bloqueio de porta de switch, consulte Usar bloqueio de porta de switch.

### Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do XenServer, consulte Criar um catálogo do XenServer

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com ambientes de nuvem do Google

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

> **Nota:**

> Antes de criar uma conexão com ambientes de nuvem do Google, você precisa primeiro concluir a configuração da sua conta do Google Cloud como um local de recurso. Consulte Ambientes do Google Cloud.

### Adicionar uma conexão

Siga as orientações em Criar uma conexão e recursos. A descrição a seguir o guiará pela configuração de uma conexão de hospedagem:

1. Em **Gerenciar > Configuração**, selecione **Hospedagem** no painel esquerdo.
2. Selecione **Adicionar Conexão e Recursos** na barra de ações.
3. Na página **Conexão**, selecione **Criar uma nova Conexão** e **ferramentas de provisionamento Citrix™**, e então selecione **Avançar**.
   - **Tipo de conexão**. Selecione **Google Cloud** no menu.
   - **Nome da conexão**. Digite um nome para a conexão.
4. Na página **Região**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Avançar**.
5. Na página **Rede**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Avançar**. O nome do recurso ajuda a identificar a combinação de região e rede. Redes virtuais com o sufixo *(Compartilhado)* anexado ao seu nome representam VPCs compartilhadas. Se você configurar uma função IAM no nível da sub-rede para uma VPC compartilhada, apenas sub-redes específicas da VPC compartilhada aparecerão na lista de sub-redes.

   > **Nota:**
   >
   > - O nome do recurso pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

6. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir** para sair da janela **Adicionar Conexão e Recursos**.

Após criar a conexão e os recursos, a conexão e os recursos criados são listados. Para configurar a conexão, selecione a conexão e, em seguida, selecione a opção aplicável na barra de ações.

Da mesma forma, você pode excluir, renomear ou testar os recursos criados sob a conexão. Para fazer isso, selecione o recurso sob a conexão e, em seguida, selecione a opção aplicável na barra de ações.

### URLs de endpoint de serviço

Você deve ter acesso às seguintes URLs:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

### Projetos do Google Cloud

Existem basicamente dois tipos de projetos do Google Cloud:

- Projeto de provisionamento: Neste caso, a conta de administrador atual é proprietária das máquinas provisionadas no projeto. Este projeto também é conhecido como projeto local.
- Projeto VPC Compartilhada: Projeto no qual as máquinas criadas no projeto de provisionamento usam a VPC do projeto VPC Compartilhada. A conta de administrador usada para o projeto de provisionamento tem permissões limitadas neste projeto, especificamente, apenas permissões para usar a VPC.

### Criar um ambiente seguro para tráfego gerenciado pelo GCP

Você pode permitir o acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aprimora a segurança para manipular dados confidenciais. Para conseguir isso, você pode fazer uma das seguintes ações:

- Inclua as seguintes regras de entrada dos controles de serviço de VPC para a Conta de Serviço do Cloud Build. Se você fizer esta etapa, não siga as etapas abaixo para criar um ambiente seguro para o tráfego gerenciado pelo GCP.

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed
```

```
To:

Projects =

All projects

Services =

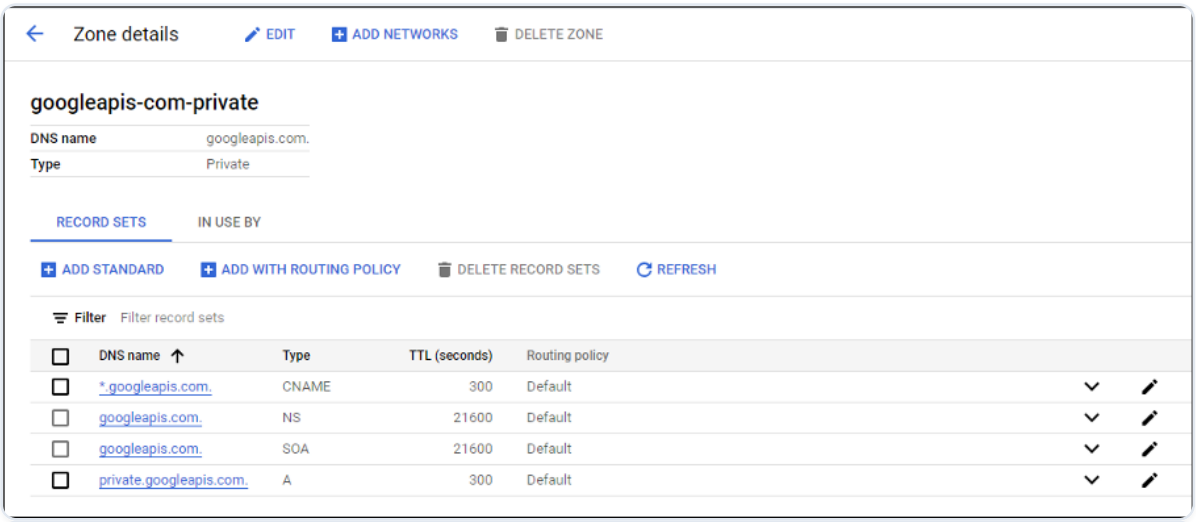
Service name: All services
```

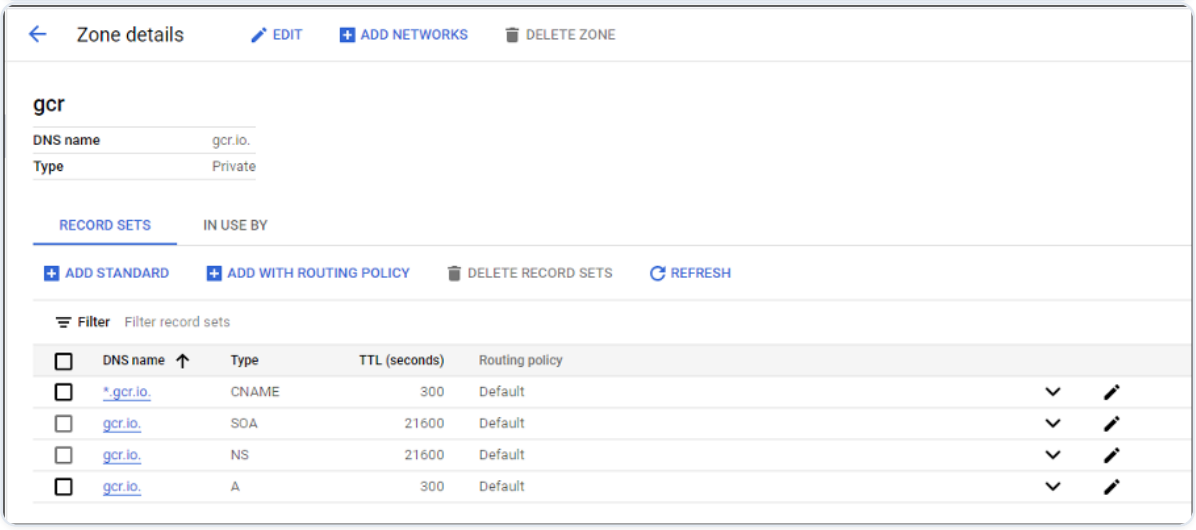
- Se você estiver usando um pool de trabalhadores privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter informações sobre o pool de trabalhadores privado, consulte Visão geral de pools privados.

**Requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP**

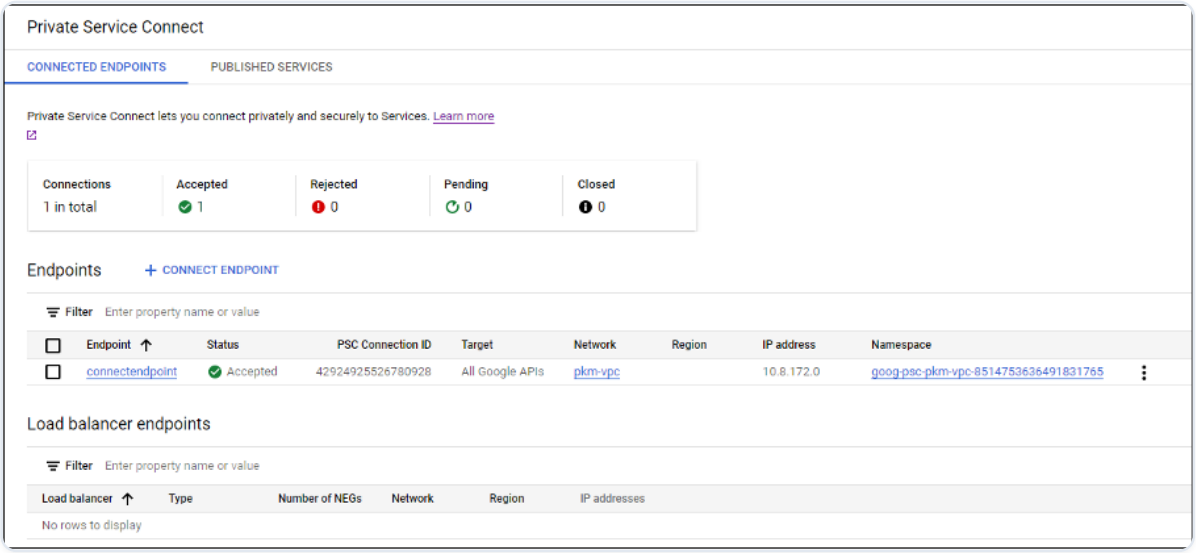
Os requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP são:

- Certifique-se de que a conexão de hospedagem esteja no modo de manutenção ao atualizar as propriedades personalizadas.
- Para usar pools de trabalhadores privados, as seguintes alterações são necessárias:
  - Para a Conta de Serviço do Citrix Cloud™, adicione as seguintes funções IAM:
    - Conta de Serviço do Cloud Build
    - Administrador de Instância de Computação
    - Usuário da Conta de Serviço
    - Criador de Token da Conta de Serviço
    - Proprietário do WorkerPool do Cloud Build
  - Crie a Conta de Serviço do Citrix Cloud no mesmo projeto que você usa para criar uma conexão de hospedagem.
  - Configure zonas DNS para `private.googleapis.com` e `gcr.io` conforme descrito em Configuração de DNS.

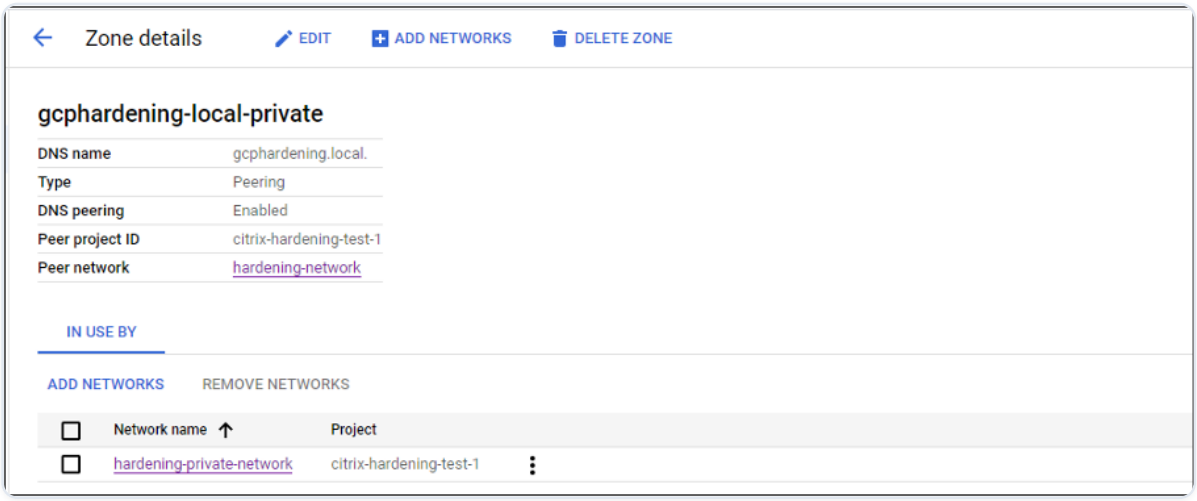



- Configure a Tradução de Endereços de Rede (NAT) privada ou use a conexão de serviço privada. Para obter mais informações, consulte Acessar APIs do Google por meio de endpoints.



- Se estiver usando uma VPC emparelhada, crie um emparelhamento de zona do Cloud DNS para a VPC emparelhada. Para obter mais informações, consulte Criar uma zona de emparelhamento.




- Nos controles de serviço da VPC, configure regras de Egress para que as APIs e VMs possam se comunicar com a internet. As regras de Ingress são opcionais. Por exemplo:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

### Habilitar o pool de trabalhadores privado

Para habilitar o pool de trabalhadores privado, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell no host do Delivery Controller ou use o SDK do PowerShell Remoto. Para obter mais informações sobre o SDK do PowerShell Remoto, consulte SDKs e APIs.

2. Execute os seguintes comandos:

   a. `Add-PSSnapin citrix*`

   b. `cd XDHyp:\Connections\`

   c. `dir`

3. Copie o `CustomProperties` da conexão para um bloco de notas.

4. Anexe a configuração da propriedade `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`. Por exemplo:

   ```
   ```

   <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

   <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
   Value="True"/>

   </CustomProperties>

   ```
   ```

5. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo: `$customProperty = '<CustomProperties…</CustomProperties>'`.

6. Execute `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.

7. Execute `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.

8. Execute `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.

9. Execute o seguinte para atualizar uma conexão de host existente:

   ```
   Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
   NAME HERE>') -SecurePassword $securePassword -UserName
   $gcpServiceAccount -CustomProperties $customProperty
   ```

### Permissões GCP necessárias

Esta seção contém a lista completa de permissões do GCP. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

> **Nota:**
>
> O GCP está introduzindo alterações no comportamento padrão e no uso de contas de serviço do Cloud Build Services após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build ativada antes de April 29, 2024 não são afetados por esta alteração. No entanto, se você quiser ter o comportamento existente do Cloud Build Service após April 29, poderá criar ou aplicar a política da organização para desativar a imposição da restrição antes de ativar a API. Se você definir a nova política da organização, ainda poderá seguir as permissões existentes nesta seção e os itens que estão marcados como **Antes da Alteração da Conta de Serviço do Cloud Build**. Caso contrário, siga as permissões existentes e os itens que estão marcados como **Após a Alteração da Conta de Serviço do Cloud Build**.

#### Criando uma conexão de host

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para Shared VPC para a Conta de Serviço do Citrix Cloud no projeto Shared VPC:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação

**Gerenciamento de energia de VMs**

Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento no caso de catálogos somente com gerenciamento de energia:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get
```

```
compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

**Criar, atualizar ou excluir VMs**

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list
```

```
compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk
```

```
compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete
```

```
compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

```
compute.networks.get

compute.resourcePolicies.use
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Citrix Cloud no projeto de VPC Compartilhada para criar uma unidade de hospedagem usando VPC e sub-rede do projeto de VPC Compartilhada:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário do Cloud Datastore

Permissões mínimas necessárias ao baixar o disco de instruções de preparação para o MCS:

- (Antes da alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Build no projeto de provisionamento.
- (Após a alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount
```

```
compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Conta de Serviço do Cloud Build (Após a alteração da Conta de Serviço do Cloud Build, é a Conta de Serviço do Cloud Compute)
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

- Permissões mínimas necessárias para a Conta de Serviço do Cloud Compute no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário da Conta de Armazenamento
- Usuário do Cloud Datastore

Permissões adicionais necessárias para VPC Compartilhada ao baixar o disco de instruções de preparação para o MCS:

- (Antes da alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Build no projeto de provisionamento.
- (Após a alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

```
compute.firewalls.list

compute.networks.list
```

```
compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

Os seguintes papéis definidos pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário da Conta de Armazenamento
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para o Cloud Key Management Service (KMS) para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

Os seguintes papéis definidos pelo Google têm as permissões listadas acima:

- Visualizador de KMS de Computação

**Permissões gerais**

A seguir estão as permissões para a conta de serviço do Citrix Cloud no projeto de provisionamento para todos os recursos suportados no MCS. Essas permissões fornecem a melhor compatibilidade daqui para frente:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list
```

```
compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete
```

```
compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity
```

```
compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list
```

```
compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs
```

```
compute.resourcePolicies.use
```

### Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas da Google Cloud Platform (GCP), consulte Criar um catálogo do Google Cloud Platform

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com HPE Moonshot

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do HPE Moonshot.

> **Observação:**
>
> Antes de criar uma conexão com o HPE Moonshot, você precisa primeiro concluir a configuração da sua conta HPE. Consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/hpe-moonshot.html).

### Criar uma conexão

Você pode criar uma conexão com o HPE Moonshot usando:

- Web Studio
- Comandos PowerShell

#### Criar uma conexão usando o Web Studio

1. Na página **Adicionar Conexão e Recursos**, selecione **HPE Moonshot** como o tipo de conexão.
2. Insira o endereço de conexão do seu Moonshot iLO Chassis Manager. Você pode usar um endereço IP, nome de host ou FQDN para o endereço.

3. Insira suas credenciais administrativas do chassi e um nome de conexão amigável.

A configuração da conexão para quando uma das seguintes situações ocorre:

- O Citrix Virtual Apps and Desktops™ recebe um certificado público assinado por CA com erros: Uma mensagem de erro aparece. Siga as instruções na tela para corrigir o problema. Caso contrário, você não poderá prosseguir com a criação da conexão.
- O Citrix Virtual Apps and Desktops recebe um certificado privado assinado por CA. Uma página de aviso aparece. Compare a impressão digital recebida com a do servidor para a validade do certificado. Se for válido, selecione **Confiar no certificado** e clique em **OK** para prosseguir com a criação da conexão. O Citrix Virtual Apps and Desktops confiará então no certificado e armazenará a impressão digital para validação futura.

### Criar uma conexão usando comandos PowerShell

Ao criar uma conexão usando o comando PowerShell, forneça as seguintes informações:

- IP: Endereço IP do Servidor HPE
- Nome de usuário: Nome de usuário HPE
- Senha: Senha HPE

Por exemplo:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

**Observação:**

O parâmetro `sslthumbprint` é necessário apenas para certificados assinados por CA privada.

### Validação de certificado e impressão digital

Para criar uma conexão bem-sucedida com o **HPE Moonshot**, o certificado não deve ter erros e a impressão digital deve ter um valor correto. A seguir estão os casos de uso relacionados à validação de certificado e impressão digital:

- O certificado assinado por CA pública tem erros. A conexão não é criada com sucesso. Consulte os detalhes do erro e resolva o problema.
- Certificado assinado por CA pública sem erros. A conexão é criada com sucesso e o valor `SslThumbprints` é **Null**.
- Certificado assinado por CA privada sem erros e um valor `sslthumbprint`. A conexão é criada com sucesso com um valor `SslThumbprints` correto.
- Certificado assinado por CA privada com um valor de thumbprint incorreto. A conexão não é criada com sucesso.
- Certificado assinado por CA privada sem erros. A conexão é criada com sucesso. O `SSlThumbprints` é **Null** ao criar a conexão. O valor `SSlThumbprints` é atualizado para um valor pelo serviço do site.

### Gerenciar conexões

Esta seção detalha como você pode gerenciar conexões:

- Corrigir problemas de certificado usando o Web Studio
- Atualizar valor de thumbprint usando o comando PowerShell

#### Corrigir problemas de certificado

O Citrix Virtual Apps and Desktops bloqueia uma conexão HPE Moonshot quando surgem problemas de certificado, impedindo que você entregue e gerencie cargas de trabalho em nós HPE Moonshot associados. Você verá um ícone de erro ao lado da conexão na lista **Conexões de host**. Consulte a tabela a seguir para problemas e soluções específicas.

| PROBLEMA | SOLUÇÃO |
| --- | --- |
| Ocorre um erro de certificado no certificado assinado por CA pública | Clique na conexão e selecione a guia **Solução de problemas**. Visualize os detalhes do erro e resolva o problema. |

| PROBLEMA | SOLUÇÃO |
| --- | --- |
| O certificado recebido é assinado por CA privada ou expirou. | Edite a conexão do host para atualizar a impressão digital do certificado. Etapas detalhadas:<br>1. Selecione a conexão e clique em **Editar Conexão**.<br>2. Na página **Propriedades da Conexão**, clique em **Editar configurações**.<br>3. Digite a senha para se conectar ao chassi HPE Moonshot e clique em **Salvar**.<br>4. Na página de **Aviso** que aparece, compare a impressão digital recebida com a do servidor para validar o certificado.<br>5. Se forem iguais, selecione **Confiar no certificado** e clique em **OK**. |

### Atualizar valores de impressão digital

Após criar a conexão, você pode atualizar o valor de thumbprint de uma conexão usando o comando PowerShell `Set-Item`. Por exemplo, execute os seguintes comandos:

1. Obtenha os detalhes de conexão de uma conexão. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. Atualize o valor da impressão digital. Por exemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Verifique o valor da impressão digital atualizado. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

**Observação:**

A atualização falha se você fornecer um valor de impressão digital incorreto no comando `Set-Item`.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do AWS, consulte Criar um catálogo de máquinas HPE Moonshot

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com o Microsoft Azure

**Observação:**

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

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Azure Resource Manager.

> **Observação:**

> Antes de criar uma conexão com o Microsoft Azure, você deve concluir a configuração da sua conta do Azure como um local de recurso. Consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

### Criar entidades de serviço e conexões

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

- Crie um principal de serviço e uma conexão juntos usando o Web Studio
- Criar uma conexão usando uma entidade de serviço criada anteriormente

Esta seção mostra como concluir estas tarefas:

- Criar um principal de serviço e conexão usando o Web Studio
- Criar uma entidade de serviço usando o PowerShell
- Obter o segredo do aplicativo no Azure
- Criar uma conexão usando uma entidade de serviço existente

#### Considerações

- A Citrix® recomenda usar o Principal de Serviço com a função de colaborador. No entanto, consulte a seção Permissões mínimas para obter a lista de permissões mínimas.
- Ao criar a primeira conexão, o Azure solicita que você conceda as permissões necessárias. Para futuras conexões, você ainda deve autenticar, mas o Azure se lembrará do seu consentimento anterior e não exibirá o prompt novamente.
- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- A conta usada para autenticação deve ser membro do diretório da assinatura. Existem dois tipos de contas a serem observados: 'Work or School' e 'personal Microsoft account'. Consulte CTX219211 para obter detalhes.
- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, podem ocorrer complicações se o usuário tiver recebido anteriormente

acesso de convidado a um dos recursos do diretório. Nesse caso, ele pode ter uma entrada de espaço reservado no diretório que não concede as permissões necessárias, e um erro é retornado.

Corrija isso removendo os recursos do diretório e adicionando-os novamente explicitamente. No entanto, use esta opção com cuidado, pois ela pode ter efeitos indesejados para outros recursos que a conta pode acessar.

- Existe um problema conhecido em que certas contas são detectadas como convidados do diretório quando na verdade são membros. Configurações como essa geralmente ocorrem com contas de diretório mais antigas e estabelecidas. Solução alternativa: adicione uma conta ao diretório, que assume o valor de associação adequado.
- Grupos de recursos são simplesmente contêineres para recursos, e eles podem conter recursos de regiões diferentes da sua própria região. Isso pode ser potencialmente confuso se você esperar que os recursos exibidos na região de um grupo de recursos estejam disponíveis.
- Certifique-se de que sua rede e sub-rede sejam grandes o suficiente para hospedar o número de máquinas que você precisa. Isso requer alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientação sobre a capacidade do espaço de endereço.

### Criar um principal de serviço e conexão usando o Web Studio

> **Importante:**
>
> Este recurso ainda não está disponível para assinaturas do Azure China.

> Com o Web Studio, você pode criar um principal de serviço e uma conexão em um único fluxo de trabalho. Principais de serviço concedem às conexões acesso aos recursos do Azure. Quando você autenticar no Azure para criar um principal de serviço, um aplicativo é registrado no Azure. Uma chave secreta (chamada de segredo do cliente ou segredo do aplicativo) é criada para o aplicativo registrado. O aplicativo registrado (uma conexão neste caso) usa o segredo do cliente para autenticar no Azure AD.

Antes de começar, certifique-se de ter cumprido estes pré-requisitos:

- Você tem uma conta de usuário no locatário do Azure Active Directory da sua assinatura.

- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativo para autenticação. Essas permissões podem ser revogadas após a criação da conexão do host. Para obter mais informações sobre funções, consulte Funções internas do Azure AD.

Use o assistente **Adicionar Conexão e Recursos** para criar um principal de serviço e uma conexão juntos:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, insira o ID da sua assinatura do Azure e um nome para a conexão. Depois de inserir o ID da assinatura, o botão **Criar novo** é ativado.

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

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

   > **Observação:**

> Depois de autenticar com sucesso no Azure, os botões **Criar novo** e **Usar existente** desaparecem. O texto **Conexão bem-sucedida** aparece, com uma marca de seleção verde, indicando a conexão bem-sucedida à sua assinatura do Azure.

8. Na página **Detalhes da Conexão**, selecione **Avançar**.

> **Observação:**
>
> Você não pode prosseguir para a próxima página até que autenticar com sucesso no Azure e consinta em conceder as permissões necessárias.

9. Configure os recursos para a conexão. Os recursos compreendem a região e a rede.
   - Na página **Região**, selecione uma região.
   - Na página **Rede**, faça o seguinte:
     - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.
     - Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.
10. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

#### EXIBIR O ID DO APLICATIVO

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

Na lista **Adicionar Conexão e Recursos**, selecione a conexão para visualizar os detalhes. A guia **Detalhes** mostra o ID do Aplicativo.

### Criar um principal de serviço usando PowerShell

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

Certifique-se de ter estes itens prontos:

- **SubscriptionId:** `SubscriptionID` do Azure Resource Manager para a assinatura onde você deseja provisionar VDAs.
- **ActiveDirectoryID**: ID do locatário do aplicativo que você registrou no Azure AD.
- **ApplicationName:** Nome do aplicativo a ser criado no Azure AD.

As etapas detalhadas são as seguintes:

Conecte-se à sua assinatura do Azure Resource Manager.

```
`Connect-AzAccount`
```

1. Selecione a assinatura do Azure Resource Manager onde você deseja criar o service principal.

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

2. Crie o aplicativo em seu locatário do AD.

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

3. Crie um service principal.

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

4. Atribua uma função ao service principal.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. Na janela de saída do console do PowerShell, anote o ApplicationId. Você fornece esse ID ao criar a conexão de host.

**Obtenha o segredo do aplicativo no Azure**

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

As etapas detalhadas são as seguintes:

1. Obtenha o **ID do Aplicativo** no Web Studio ou usando o PowerShell.
2. Faça login no portal do Azure.
3. No Azure, selecione **Azure Active Directory**.
4. Em **Registros de aplicativo** no Azure AD, selecione seu aplicativo.

5. Vá para **Certificados e segredos**.
6. Clique em **Segredos do cliente**.

### Criar uma conexão usando 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 estes itens prontos:

- SubscriptionId
- ActiveDirectoryID (ID do locatário)
- ID do Aplicativo
- Segredo do aplicativo

  Para obter mais informações, consulte Obter o segredo do aplicativo.
- Data de expiração do segredo

As etapas detalhadas são as seguintes:

No assistente **Adicionar Conexão e Recursos**:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, insira seu ID de assinatura do Azure e um nome para a conexão.

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

4. Selecione **Usar existente**. Na janela **Detalhes do Principal de Serviço Existente**, insira as seguintes configurações para o principal de serviço existente. Depois de inserir os detalhes, o botão **Salvar** é ativado. Selecione **Salvar**. Você não pode prosseguir além desta página até fornecer detalhes válidos.

- **ID da Assinatura**. Insira seu ID de assinatura do Azure. Para obter seu ID de assinatura, faça login no portal do Azure e navegar para **Assinaturas > Visão geral**.
- **ID do Active Directory** (ID do locatário). Insira o ID do Diretório (locatário) do aplicativo que você registrou no Azure AD.
- **ID do Aplicativo**. Insira o ID do Aplicativo (cliente) do aplicativo que você registrou no Azure AD.
- **Segredo do aplicativo**. Crie uma chave secreta (segredo do cliente). O aplicativo registrado usa a chave para autenticar no Azure AD. Recomendamos que você altere as chaves regularmente por motivos de segurança. Certifique-se de salvar a chave, pois você não poderá recuperá-la mais tarde.
- **Data de expiração do segredo**. Insira a data após a qual o segredo do aplicativo expira. Você verá um ícone de aviso na conexão de host específica no nó **Hospedagem** a partir de 14 dias antes da expiração da chave secreta. No entanto, se a chave secreta expirar, você receberá erros.

> **Observação:**
>
> Para fins de segurança, o período de expiração não pode ser superior a dois anos a partir de agora.

- **URL de autenticação**. Este campo é preenchido automaticamente e não é editável.
- **URL de gerenciamento**. Este campo é preenchido automaticamente e não é editável.
- **Sufixo de armazenamento**. Este campo é preenchido automaticamente e não é editável.

  O acesso aos seguintes endpoints é necessário para criar um catálogo MCS no Azure. O acesso a esses endpoints otimiza a conectividade entre sua rede e o portal do Azure e seus serviços.

  - URL de autenticação: `<https://login.microsoftonline.com/>`
  - URL de gerenciamento: `<https://management.azure.com/>`. Esta é uma URL de solicitação para APIs do provedor do Azure Resource Manager. O endpoint para gerenciamento depende do ambiente. Por exemplo, para o Azure Global, é `<https://management.azure.com/>`, e para o Azure US Government, é `<https://management.usgovcloudapi.net/>`.

- Sufixo de armazenamento: `<https://*.core.windows.net./>`. Este (*) é um caractere curinga para sufixo de armazenamento. Por exemplo, `https://demo.table.core.windows.net/`.

5. Após selecionar **Salvar**, você retorna à página **Detalhes da Conexão**. Selecione **Avançar** para continuar para a próxima página.
6. Configure os recursos para a conexão. Os recursos compreendem a região e a rede.
   - Na página **Região**, selecione uma região.
   - Na página **Rede**, faça o seguinte:
     - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.
     - Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.
7. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

## Gerenciar entidades de serviço e conexões

Esta seção detalha como você pode gerenciar entidades de serviço e conexões:

- Configurar as configurações de limitação do Azure
- Habilitar o compartilhamento de imagens no Azure
- Adicionar locatários compartilhados a uma conexão usando o Web Studio
- Implementar o compartilhamento de imagens usando o PowerShell
- Gerenciar o segredo do aplicativo e a data de expiração do segredo

### Configurar as definições de limitação do Azure

O Azure Resource Manager limita as solicitações para assinaturas e locatários, roteando o tráfego com base em limites definidos, adaptados às necessidades específicas do provedor. Consulte Limitação de solicitações do Resource Manager no site da Microsoft para obter mais informações. Existem limites para assinaturas e locatários, onde o gerenciamento de muitas máquinas pode se

tornar problemático. Por exemplo, uma assinatura que contém muitas máquinas pode apresentar problemas de desempenho relacionados a operações de energia.

**Dica:**

Para obter mais informações, consulte Melhorando o desempenho do Azure com o Machine Creation Services.

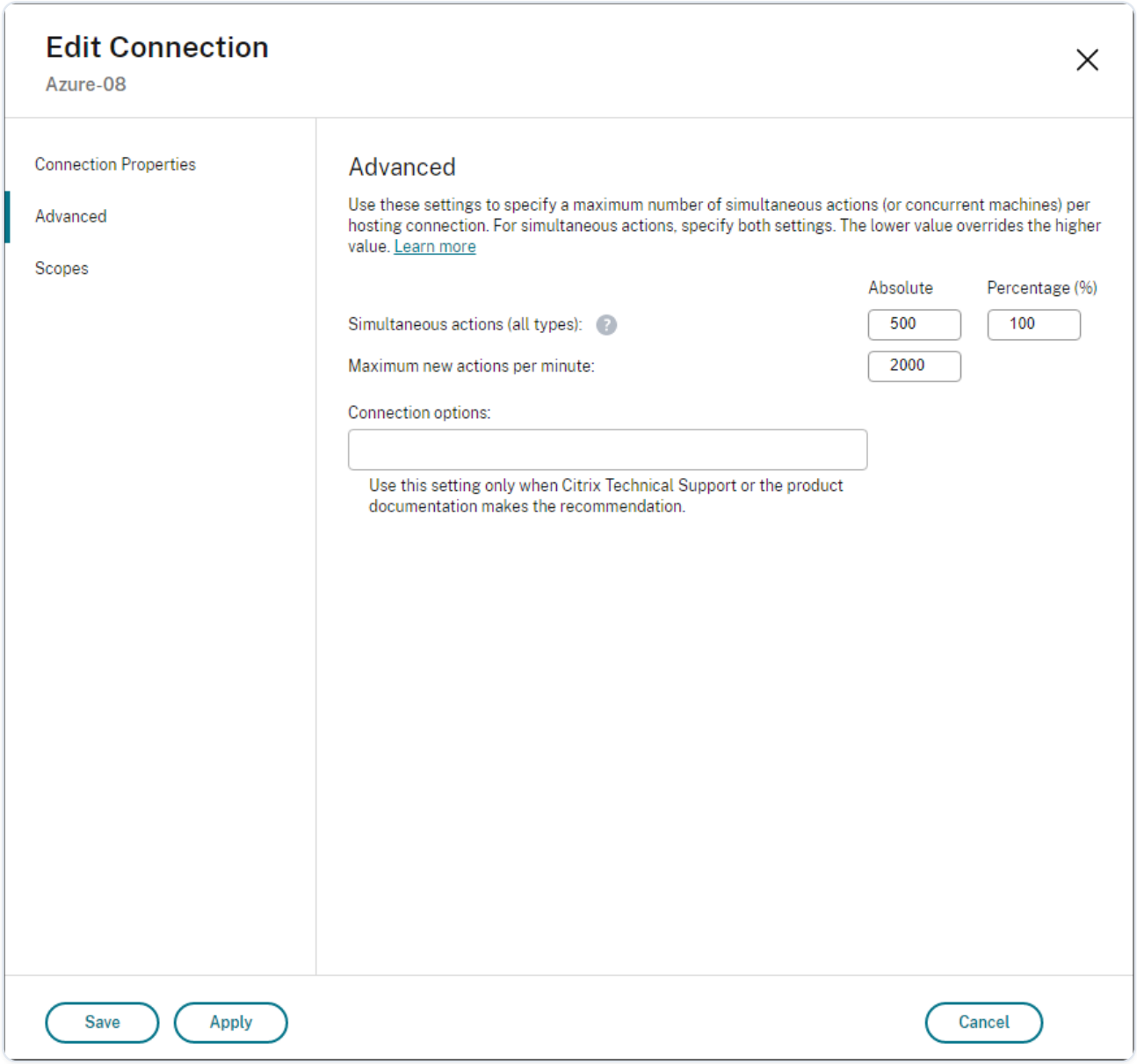
Para ajudar a mitigar esses problemas, você pode remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

Recomendamos as seguintes configurações ideais ao ligar ou desligar VMs em grandes assinaturas, por exemplo, aquelas que contêm 1.000 VMs:

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

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

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




O MCS suporta um máximo de 500 operações simultâneas por padrão. Alternativamente, você pode usar o SDK do PowerShell Remoto para definir o número máximo de operações simultâneas.

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

- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` usando o comando PowerShell `Set-item`.

### Habilitar o compartilhamento de imagens no Azure

Ao criar ou atualizar catálogos de máquinas, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas através da Galeria de Computação do Azure). Para habilitar o compartilhamento de imagens dentro ou entre locatários, você deve fazer as configurações necessárias no Azure:

- Compartilhar imagens dentro de um locatário (entre assinaturas)
- Compartilhar imagens entre locatários

#### COMPARTILHAR IMAGENS DENTRO DE UM LOCATÁRIO (ENTRE ASSINATURAS)

Para selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura diferente, a imagem deve ser compartilhada com o principal de serviço (SPN) dessa assinatura.

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

Principal de serviço: SPN 1

Assinatura: subscription 1

Locatário: tenant 1

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

Assinatura: subscription 2

Locatário: tenant 1

Se você quiser compartilhar a imagem na assinatura 2 com a assinatura 1 (SPN 1), vá para a assinatura 2 e compartilhe o grupo de recursos com o SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em função do Azure (RBAC). O RBAC do Azure é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o RBAC do Azure, consulte o documento da Microsoft O que é o controle de acesso baseado em função do Azure (RBAC do Azure). Para conceder acesso, você atribui funções a entidades de serviço no escopo do grupo de recursos com a função de Colaborador. Para atribuir funções do Azure, você deve ter a permissão `Microsoft.Authorization/roleAssignments/write`, como Administrador de Acesso do Usuário ou Proprietário. Para obter mais informações sobre como compartilhar imagens com outro SPN, consulte o documento da Microsoft Atribuir funções do Azure usando o portal do Azure.

Para obter informações sobre como selecionar uma imagem de uma assinatura diferente usando comandos do PowerShell, Selecione uma imagem de uma assinatura diferente.

### COMPARTILHAR IMAGENS ENTRE LOCATÁRIOS

Para compartilhar imagens entre locatários com a Azure Compute Gallery, crie um registro de aplicativo.

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

1. Crie um registro de aplicativo para o Locatário 1. Para obter mais informações, consulte Criar o registro do aplicativo.
2. Conceda ao Locatário 2 acesso ao aplicativo solicitando um login usando um navegador. Substitua `Tenant2 ID` pelo ID do locatário do Locatário 1. Substitua `Application (client) ID` pelo ID do aplicativo do registro do aplicativo que você criou. Ao concluir as substituições, cole o URL em um navegador e siga os prompts de login para entrar no Locatário 2. Por exemplo:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   Para obter mais informações, consulte Conceder acesso ao Locatário 2.
3. Conceda acesso ao aplicativo ao grupo de recursos do Locatário 2. Faça login como Locatário 2 e conceda acesso ao registro do aplicativo ao grupo de recursos que contém a imagem da galeria. Para obter mais informações, consulte autenticar requests across tenants.

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

1. Atualizar propriedades personalizadas de conexão de hospedagem com IDs de locatário compartilhadas.
2. Selecionar uma imagem de um locatário diferente.

#### Adicionar locatários compartilhados a uma conexão usando o Web Studio

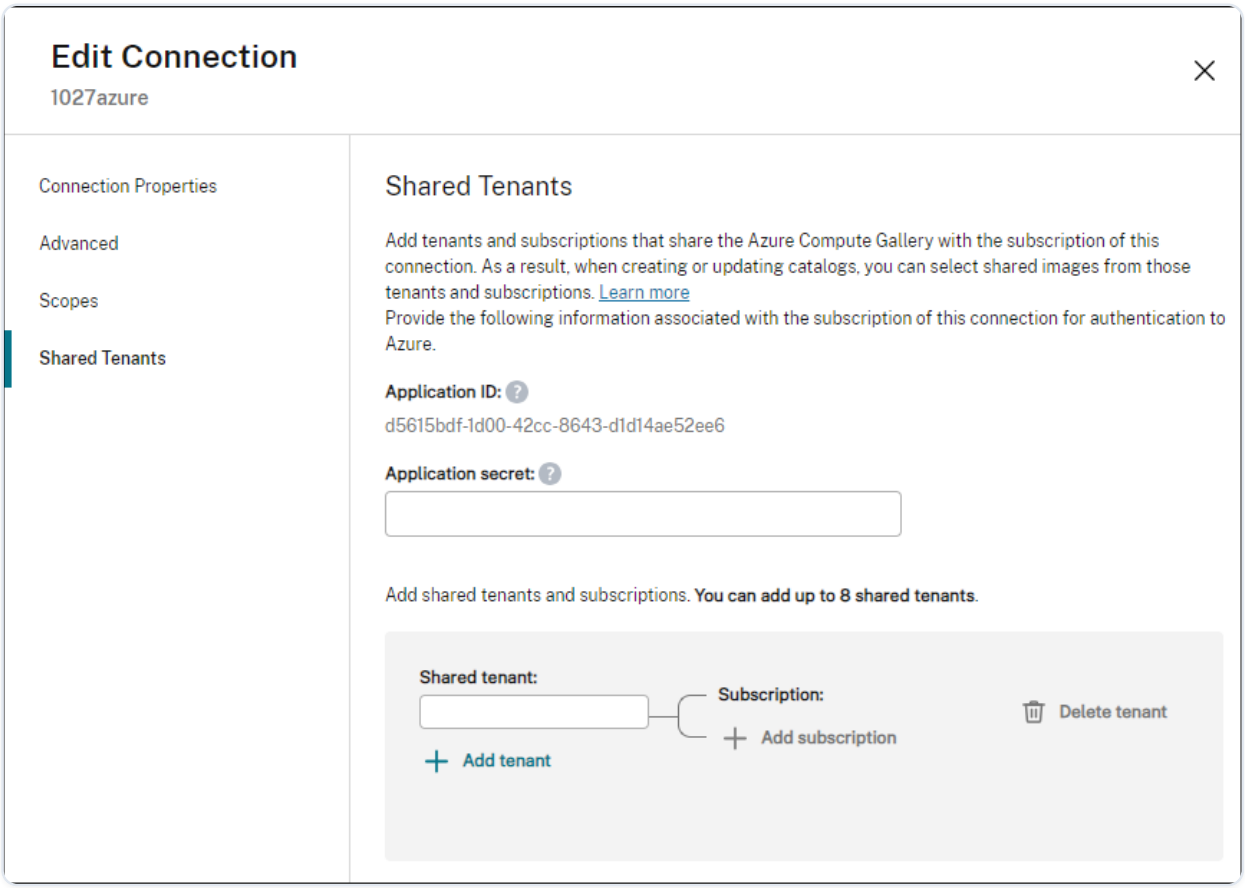
Ao criar ou atualizar catálogos de máquinas no Web Studio, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas por meio da Galeria de Computação do Azure). O recurso exige que você forneça informações de locatário e assinatura compartilhadas para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

> **Observação:**

> Certifique-se de ter configurado as configurações necessárias no Azure para habilitar o compartilhamento de imagens entre locatários. Para obter mais informações, consulte Compartilhar imagens entre locatários.

> Conclua as seguintes etapas para uma conexão:

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




3. Em **Locatários Compartilhados**, faça o seguinte:
   - Forneça o ID do aplicativo e o segredo do aplicativo associados à assinatura da conexão. O Citrix Virtual Apps and Desktops usa essas informações para autenticar no Azure AD.
   - Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura da conexão. Você pode adicionar até 8 locatários compartilhados e 8 assinaturas para cada locatário.
4. Quando terminar, selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

### Implementar o compartilhamento de imagens usando o PowerShell

Esta seção o orienta pelos processos de compartilhamento de imagens usando o PowerShell:

- Selecionar uma imagem de uma assinatura diferente
- Atualizar propriedades personalizadas de conexão de hospedagem com IDs de locatário compartilhados
- Selecionar uma imagem de um locatário diferente

#### SELECIONAR UMA IMAGEM DE UMA ASSINATURA DIFERENTE

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

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

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

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

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

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

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

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

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

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

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão de imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

### ATUALIZAR PROPRIEDADES PERSONALIZADAS DE CONEXÃO DE HOSPEDAGEM COM IDS DE LOCATÁRIO COMPARTILHADAS

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

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

Por exemplo:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

**Observação:**

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

### SELECIONE UMA IMAGEM DE UM LOCATÁRIO DIFERENTE

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

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

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

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

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

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

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

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

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

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

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

### Gerenciar o segredo do aplicativo e a data de expiração do segredo

Certifique-se de alterar o segredo do aplicativo para uma conexão antes que o segredo expire. Você verá um ícone de aviso na conexão de host específica no nó **Hosting** a partir de 14 dias antes da expiração da chave secreta. No entanto, se a chave secreta expirar, você receberá erros.

### CRIAR UM SEGREDO DE APLICATIVO NO AZURE

Você pode criar um segredo de aplicativo para uma conexão através do portal do Azure.

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

> **Nota:**
>
> Certifique-se de salvar o segredo do cliente, pois você não poderá recuperá-lo mais tarde.

6. Copie o valor do segredo do cliente e a data de expiração.
7. No Web Studio, edite a conexão correspondente e substitua o conteúdo nos campos **Segredo do aplicativo** e **Data de expiração do segredo** pelos valores que você copiou.

### ALTERAR A DATA DE EXPIRAÇÃO DO SEGREDO

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

> **Nota:**
>
> Você verá um ícone de aviso na conexão de host específica no nó **Hosting** a partir de 14 dias antes da expiração da chave secreta.

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

## Permissões do Azure necessárias

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

### Permissões mínimas

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

#### CRIANDO UMA CONEXÃO DE HOST

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

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

#### GERENCIAMENTO DE ENERGIA DE VMS

Ligue ou desligue as instâncias da máquina.

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

#### CRIAR, ATUALIZAR OU EXCLUIR VMS

Crie um catálogo de máquinas, adicione, exclua, atualize máquinas e exclua o catálogo de máquinas.

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

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",
```

```
"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

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

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

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

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

  ```
  "Microsoft.Compute/galleries/read",

  "Microsoft.Compute/galleries/images/read",

  "Microsoft.Compute/galleries/images/versions/read",
  ```

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

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",

  "Microsoft.Storage/storageAccounts/write",

  "Microsoft.Storage/storageAccounts/delete",
  ```

- Se você usar um grupo de recursos gerenciado pela Citrix:

  ```
  "Microsoft.Resources/subscriptions/resourceGroups/write",

  "Microsoft.Resources/subscriptions/resourceGroups/delete",
  ```

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

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

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

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- Se você usar Criptografia do Lado do Servidor (SSE) com Chaves Gerenciadas pelo Cliente (CMK):

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

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

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",
```

```
"Microsoft.Resources/deployments/delete",
```

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

```
"Microsoft.Resources/templateSpecs/read",

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

### CRIANDO, ATUALIZANDO E EXCLUINDO MÁQUINAS COM DISCO NÃO GERENCIADO

A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é VHD e o grupo de recursos é fornecido pelo administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",
```

```
"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action"
```

### Permissão geral

A função de Colaborador tem acesso total para gerenciar todos os recursos. Este conjunto de permissões não o impede de obter novos recursos.

O seguinte conjunto de permissões oferece a melhor compatibilidade daqui para frente, embora inclua mais permissões do que o necessário com o conjunto de recursos atual:

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

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",
```

```
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
```

```
"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Resources/templateSpecs/read",

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

### Configurar as permissões necessárias para a conexão de host do Azure

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

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

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

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do Azure, consulte Criar um catálogo do Microsoft Azure

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com o Microsoft System Center Virtual Machine Manager

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Microsoft System Center Virtual Machine Manager (VMM).

> **Observação:**
>
> Antes de criar uma conexão com o VMM, você precisa primeiro concluir a configuração da sua conta VMM como um local de recurso. Consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

### Criar uma conexão

Se você usou o MCS para provisionar VMs, faça o seguinte no assistente de criação de conexão:

- Insira o endereço como um nome de domínio totalmente qualificado do servidor host.

- Insira as credenciais para a conta de administrador que você configurou anteriormente. Esta conta deve ter permissão para criar novas VMs.
- Na caixa de diálogo Detalhes do Host, selecione o cluster ou host autônomo a ser usado ao criar VMs.

> **Importante**
>
> Procure um cluster ou host autônomo mesmo se você estiver usando uma implantação de host Hyper-V único.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para criar catálogos de máquinas com MCS em compartilhamento de arquivos SMB 3, consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com Nutanix

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Nutanix.

> **Nota:**
>
> Antes de criar uma conexão com o Nutanix, você precisa primeiro concluir a configuração da sua conta Nutanix como um local de recurso. Consulte Ambientes de virtualização Nutanix.

### Criar uma conexão com o Nutanix

As informações a seguir são um suplemento às orientações em Conexões e recursos. Para criar uma conexão Nutanix, siga as orientações gerais desse artigo, observando os detalhes específicos do Nutanix.

No assistente **Adicionar Conexão e Recursos**, selecione o tipo de conexão Nutanix na página **Conexão** e, em seguida, especifique o endereço e as credenciais, além de um nome para a conexão. Na página **Rede**, selecione uma rede para a unidade de hospedagem.

Os seguintes tipos de conexão estão disponíveis para seleção: **Nutanix AHV**, **Nutanix AHV DRaaS** e **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique o endereço e as credenciais do cluster Prism Element (PE).
- Para **Nutanix AHV PC**, especifique o endereço e as credenciais do Prism Central (PC).

> **Observação:**
>
> Atualmente, o tipo de conexão Nutanix AHV PC é usado apenas para criar conexão com o Nutanix Cloud Cluster (NC2) no Azure. Além disso, um catálogo de máquinas só pode ser hospedado em um único cluster em uma conexão NC2 no Azure.

- Para **Nutanix AHV DRaaS**, especifique o endereço e o nome de usuário do locatário DRaaS. Importe seus arquivos de credenciais privados e públicos do Nutanix DRaaS (`.pem`).

> **Dica:**
>
> Se você implantar máquinas usando o Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do Nutanix, consulte Criar um catálogo Nutanix

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com a nuvem Nutanix e soluções de parceiros

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos da nuvem Nutanix e das soluções de parceiros.

O Citrix Virtual Apps and Desktops™ oferece suporte à seguinte solução de nuvem e parceira Nutanix:

- Clusters de Nuvem Nutanix no AWS

> **Observação:**
>
> Antes de criar uma conexão com a solução de nuvem e parceira Nutanix, você precisa primeiro concluir a configuração de sua respectiva conta como um local de recurso. Consulte Soluções de nuvem e parceiras Nutanix.

### Conectar-se ao Nutanix Prism

Depois de criar um cluster Nutanix, conecte-se ao Nutanix Prism.

Para se conectar ao Nutanix Prism:

1. Crie uma VM bastion na sub-rede 10.0.129.0/24.
2. Conecte-se via RDP à VM bastion, vá para o URL do **Prism Element** que você copiou na seção anterior.
3. Faça login usando as credenciais padrão: `admin:nutanix/4u`. Lembre-se de alterar a senha.

### Crie uma VM no Cluster Nutanix

Depois de se conectar ao **Nutanix Prism**, crie VMs no cluster Nutanix.

#### Se a VM precisar de acesso à Internet

1. Vá para o console do AWS.
2. Crie uma nova sub-rede 10.0.130.0/24 na mesma VPC que a criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas desta sub-rede para direcionar todo o tráfego não local para o gateway NAT acima.
4. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
5. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a mesma sub-rede 10.0.130.0/24 usada na AWS.
6. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa nova sub-rede.

#### Se a VM não precisar de acesso à Internet

1. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
2. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a sub-rede 10.0.129.0/24.
3. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa sub-rede.

> **Dica:**
>
> Certifique-se de que as informações de hora e fuso horário nas VMs estejam configuradas corretamente. Isso é especialmente verdadeiro para o AD.

### Criar conexão de host

1. Inicie o Web Studio.
2. Selecione o nó de hospedagem e clique em **Adicionar Conexão e Recursos**.
3. Na tela **Conexão**, selecione **Criar uma nova Conexão** e, no **Endereço da conexão**, insira `https://xxx.xxx.xxx.xxx:9440`.
4. Siga a interface do usuário para concluir o assistente.

> **Observação:**
>
> Para ver a opção Nutanix no Web Studio, todas as VMs do conector devem ter o plug-in nutanix instalado, mesmo que não sejam usadas na zona nutanix.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do Nutanix, consulte Criar um catálogo Nutanix

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

# Conexão com VMware

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização VMware.

> **Observação:**
>
> Antes de criar uma conexão com o VMware, você precisa primeiro concluir a configuração da sua conta VMware como um local de recurso. Consulte Ambientes de virtualização VMware.

## Criar uma conexão

No assistente de criação de conexão:

1. Selecione o tipo de conexão VMware.
2. Especifique o endereço do ponto de acesso para o SDK do vCenter.
3. Especifique as credenciais para uma conta de usuário VMware que você configurou anteriormente e que tem permissões para criar VMs. Especifique o nome de usuário no formato domínio/nome_de_usuário.

## Impressão digital SSL do VMware

O recurso de impressão digital SSL do VMware elimina a necessidade de criar manualmente uma conexão de host com um hipervisor VMware vSphere. Não é mais necessário criar manualmente uma relação de confiança entre os Delivery Controllers no Site e o certificado do hipervisor antes de criar uma conexão.

O recurso de impressão digital SSL do VMware armazena a impressão digital do certificado não confiável no banco de dados do Site. Essa configuração garante que o hipervisor possa ser continuamente identificado como confiável pelo Citrix Virtual Apps and Desktops™, mesmo que não pelos Controllers.

Ao criar uma conexão de host vSphere no Studio, uma caixa de diálogo permite visualizar o certificado da máquina à qual você está se conectando. Você pode então escolher se deseja confiar nele.

### Privilégios necessários

Crie uma conta de usuário VMware e uma ou mais funções VMware com um conjunto ou todas as permissões listadas neste artigo. Baseie a criação das funções no nível específico de granularidade exigido sobre as permissões do usuário para solicitar as várias operações do Citrix DaaS™ a qualquer momento. Para conceder as permissões específicas do usuário a qualquer momento, associe-as à função respectiva, no nível do data center no mínimo, com a opção **Propagar para filhos** selecionada. No entanto, para as permissões `StorageProfile` e uma permissão `Tags` específica, aplique as permissões no nível do Root vCenter Server, sem **Propagar para Filhos**. Consulte as notas em cada uma dessas tabelas.

As tabelas a seguir mostram os mapeamentos entre as operações do Citrix Virtual Apps and Desktops e os privilégios mínimos necessários do VMware.

> **Observação:**
>
> O nome de exibição da lista de permissões, especificamente a *Interface do Usuário*, é diferente para algumas versões do vSphere. Por exemplo, no vSphere 6.7, a permissão *Interface do Usuário* é **Alterar Memória** e **Alterar Configurações**, em vez de **Configurações** e **Memória**, conforme descrito nos privilégios necessários nesta página.

#### Adicionar conexões e recursos

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| System. Anonymous, System. Read e System.View | Adicionado automaticamente. Pode usar a função somente leitura integrada. |

#### Gerenciamento de energia

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| VirtualMachine.Interact.PowerOff | Máquina virtual > Interação > Desligar |
| VirtualMachine.Interact.PowerOn | Máquina virtual > Interação > Ligar |
| VirtualMachine.Interact.Reset | Máquina virtual > Interação > Redefinir |
| VirtualMachine.Interact.Suspend | Máquina virtual > Interação > Suspender |

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| Datastore.Browse | Datastore > Navegar no armazenamento de dados |

### Provisionar máquinas (Machine Creation Services™)

Para provisionar máquinas usando o MCS, as seguintes permissões são obrigatórias:

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| Datastore.AllocateSpace | Datastore > Alocar espaço |
| Datastore.Browse | Datastore > Navegar no armazenamento de dados |
| Datastore.FileManagement | Datastore > Operações de arquivo de baixo nível |
| Network.Assign | Network > Atribuir rede |
| Resource.AssignVMToPool | Recurso > Atribuir máquina virtual ao pool de recursos |
| VirtualMachine.Config.AddExistingDisk | Máquina virtual > Configuração > Adicionar disco existente |
| VirtualMachine.Config.AddNewDisk | Máquina virtual > Configuração > Adicionar novo disco |
| Virtual machine.Config.Adicionar ou remover dispositivo | Máquina virtual > Configuração > Adicionar ou remover dispositivo |
| VirtualMachine.Config.AdvancedConfig | Máquina virtual > Configuração > Avançado |
| VirtualMachine.Config.RemoveDisk | Máquina virtual > Configuração > Remover disco |
| VirtualMachine.Config.CPUCount | Máquina virtual > Configuração > Alterar contagem de CPU |
| VirtualMachine.Config.Memory | Máquina virtual > Configuração > Alterar memória |

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| VirtualMachine.Config.Settings | Máquina virtual > Configuração > Alterar configurações |
| VirtualMachine.Interact.PowerOff | Máquina virtual > Interação > Desligar |
| VirtualMachine.Interact.PowerOn | Máquina virtual > Interação > Ligar |
| VirtualMachine.Interact.Reset | Máquina virtual > Interação > Redefinir |
| VirtualMachine.Interact.Suspend | Máquina virtual > Interação > Suspender |
| VirtualMachine.Inventory.CreateFromExisting | Máquina virtual > Inventário > Criar a partir de existente |
| VirtualMachine.Inventory.Create | Máquina virtual > Inventário > Criar novo |
| VirtualMachine.Inventory.Delete | Máquina virtual > Inventário > Remover |
| VirtualMachine.Provisioning.Clone | Máquina virtual > Provisionamento > Clonar máquina virtual |
| VirtualMachine.State.CreateSnapshot | vSphere 5.0, Update 2, vSphere 5.1, Update 1 e vSphere 6.x, Update 1: Máquina virtual > Estado > Criar instantâneo; vSphere 5.5: Máquina virtual > Gerenciamento de instantâneos > Criar instantâneo |

### Atualização e reversão de imagem

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| Datastore.AllocateSpace | Datastore > Alocar espaço |
| Datastore.Browse | Datastore > Navegar no datastore |
| Datastore.FileManagement | Datastore > Operações de arquivo de baixo nível |
| Network.Assign | Rede > Atribuir rede |
| Resource.AssignVMToPool | Recurso > Atribuir máquina virtual ao pool de recursos |

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| VirtualMachine.Config.AddExistingDisk | Máquina virtual > Configuração > Adicionar disco existente |
| VirtualMachine.Config.AddNewDisk | Máquina virtual > Configuração > Adicionar novo disco |
| VirtualMachine.Config.AdvancedConfig | Máquina virtual > Configuração > Avançado |
| VirtualMachine.Config.RemoveDisk | Máquina virtual > Configuração > Remover disco |
| VirtualMachine.Interact.PowerOff | Máquina virtual > Interação > Desligar |
| VirtualMachine.Interact.PowerOn | Máquina virtual > Interação > Ligar |
| VirtualMachine.Interact.Reset | Máquina virtual > Interação > Redefinir |
| VirtualMachine.Inventory.CreateFromExisting | Máquina virtual > Inventário > Criar a partir de existente |
| VirtualMachine.Inventory.Create | Máquina virtual > Inventário > Criar novo |
| VirtualMachine.Inventory.Delete | Máquina virtual > Inventário > Remover |
| VirtualMachine.Provisioning.Clone | Máquina virtual > Provisionamento > Clonar máquina virtual |

### Excluir máquinas provisionadas

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| Datastore.Browse | Datastore > Navegar no datastore |
| Datastore.FileManagement | Datastore > Operações de arquivo de baixo nível |
| VirtualMachine.Config.RemoveDisk | Máquina virtual > Configuração > Remover disco |
| VirtualMachine.Interact.PowerOff | Máquina virtual > Interação > Desligar |
| VirtualMachine.Inventory.Delete | Máquina virtual > Inventário > Remover |

### Perfil de Armazenamento (vSAN)

Para visualizar, criar ou excluir políticas de armazenamento durante a criação de catálogos em um datastore vSAN, as seguintes permissões são obrigatórias:

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| StorageProfile.Update | ARMAZENAMENTO ORIENTADO POR PERFIL > Atualização de armazenamento orientado por perfil. Para vSphere 8: Políticas de armazenamento de VM > Atualizar políticas de armazenamento de VM |
| StorageProfile.View | ARMAZENAMENTO ORIENTADO POR PERFIL > Visualização de armazenamento orientado por perfil. Para vSphere 8: Políticas de armazenamento de VM > Visualizar políticas de armazenamento de VM |

**Observação:**

Aplique as permissões de perfil de armazenamento no nível do servidor vCenter Raiz, sem **Propagar para Filhos**.

### Tags e Atributos Personalizados

Tags e atributos personalizados permitem anexar metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e filtragem desses objetos. Para criar, editar, atribuir e excluir tags ou categorias, as seguintes permissões são obrigatórias:

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| InventoryService.Tagging.CreateTag | Marcação vSphere > Criar Tag vSphere |
| InventoryService.Tagging.CreateCategory | Marcação vSphere > Criar Categoria de Tag vSphere |
| InventoryService.Tagging.EditTag | Marcação vSphere > Editar Tag vSphere |
| InventoryService.Tagging.EditCategory | Marcação vSphere > Editar Categoria de Tag vSphere |

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| InventoryService.Tagging.DeleteTag | Marcação vSphere > Excluir Marcação vSphere |
| InventoryService.Tagging.DeleteCategory | Marcação vSphere > Excluir Categoria de Marcação vSphere |
| InventoryService.Tagging.AttachTag | Marcação vSphere > Atribuir ou Desatribuir Marcação vSphere |
| InventoryService.Tagging.ObjectAttachable | Marcação vSphere > Atribuir ou Desatribuir Marcação vSphere em Objeto |
| Global.ManageCustomFields | Global > Gerenciar atributos personalizados |
| Global.SetCustomField | Global > Definir atributo personalizado |

**Observação:**

- Quando o MCS cria um catálogo de máquinas, ele marca as VMs de destino com tags de nome especiais. Essas tags diferenciam a imagem mestre das VMs criadas pelo MCS e impedem o uso de VMs criadas pelo MCS para preparação de imagem. Você pode identificar a diferença pelo valor do atributo `XdProvisioned` no vCenter. O atributo é definido como **True** se o MCS criar VMs.
- Aplique a permissão `InventoryService.Tagging.AttachTag` no nível do Servidor vCenter Raiz, sem **Propagar para Filhos**.

### Operações criptográficas

Os privilégios de operações criptográficas controlam quem pode realizar qual tipo de operação criptográfica em qual tipo de objeto. O vSphere Native Key Provider usa os privilégios `Cryptographer.*`. As seguintes permissões mínimas são necessárias para operações criptográficas:

**Observação:**

Essas permissões são necessárias para criar catálogos de máquinas MCS com VM equipada com vTPM.

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| Cryptographer.Access | Privilégios > Todos os Privilégios > Operações criptográficas > Acesso direto |
| Cryptographer.AddDisk | Privilégios > Todos os Privilégios > Operações criptográficas > Adicionar disco |
| Cryptographer.Clone | Privilégios > Todos os Privilégios > Operações criptográficas > Clonar |
| Cryptographer.Encrypt | Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar |
| Cryptographer.EncryptNew | Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar novo |
| Cryptographer.Decrypt | Privilégios > Todos os Privilégios > Operações criptográficas > Descriptografar |
| Cryptographer.Migrate | Privilégios > Todos os Privilégios > Operações criptográficas > Migrar |
| Cryptographer.ReadKeyServersInfo | Privilégios > Todos os Privilégios > Operações criptográficas > Ler informações do KMS |

**Provisionar máquinas (Citrix Provisioning™)**

Essas permissões para clonar e implantar um modelo são necessárias para provisionar VMs usando o Assistente de Configuração do Citrix Virtual Apps and Desktops e o Assistente de Exportação de Dispositivos através do console do Citrix Provisioning. Defina as permissões ao criar uma conexão de hospedagem. Você precisa de todas as permissões de Provisionar máquinas (Machine Creation Services) e das seguintes.

| SDK | INTERFACE DO USUÁRIO |
|---|---|
| VirtualMachine.Config.AddRemoveDevice | Máquina virtual > Configuração > Adicionar ou remover dispositivo |
| VirtualMachine.Config.CPUCount | Máquina virtual > Configuração > Alterar contagem de CPU |
| VirtualMachine.Config.Memory | Máquina virtual > Configuração > Memória |
| VirtualMachine.Config.Settings | Máquina virtual > Configuração > Configurações |
| VirtualMachine.Provisioning.CloneTemplate | Máquina virtual > Provisionamento > Clonar modelo |
| VirtualMachine.Provisioning.DeployTemplate | Máquina virtual > Provisionamento > Implantar modelo |
| VApp.Export | vApp > Exportar |

**Observação:**

O `VApp.Export` é necessário para criar catálogos de máquinas MCS usando o perfil de máquina.

### Obter e importar um certificado

Para proteger as comunicações do vSphere, a Citrix® recomenda que você use HTTPS em vez de HTTP.

HTTPS requer certificados digitais. Use um certificado digital emitido por uma autoridade de certificação que atenda à política de segurança da sua organização.

Se você não puder usar um certificado digital emitido por uma autoridade de certificação, poderá usar o certificado autoassinado instalado pelo VMware. Use este método apenas se a política de segurança da sua organização permitir. Adicione o certificado VMware vCenter a cada Delivery Controller.

1. Adicione o nome de domínio totalmente qualificado (FQDN) do computador que executa o vCenter Server ao arquivo hosts nesse servidor, em `%SystemRoot%/WINDOWS/system32/`

`Drivers/etc/`. Esta etapa é necessária apenas se o FQDN do computador que executa o vCenter Server ainda não estiver presente no sistema de nomes de domínio.

2. Obtenha o certificado do vCenter usando qualquer um dos três métodos a seguir:

   **Do servidor vCenter.**

   a. Copie o arquivo rui.crt do servidor vCenter para um local acessível em seus Delivery Controllers.

   b. No Controller, navegar até o local do certificado exportado e abra o arquivo rui.crt.

   **Baixe o certificado usando um navegador da web.** Se você estiver usando o Internet Explorer, clique com o botão direito do mouse no Internet Explorer e escolha **Executar como Administrador** para baixar ou instalar o certificado.

   a. Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com)>`.

   b. Aceite os avisos de segurança.

   c. Clique na barra de endereço que exibe o erro de certificado.

   d. Visualize o certificado e clique na guia Detalhes.

   e. Selecione **Copiar para arquivo e exportar no formato .CER**, fornecendo um nome quando solicitado.

   f. Salve o certificado exportado.

   g. navegar até o local do certificado exportado e abra o arquivo .CER.

   **Importe diretamente do Internet Explorer executado como administrador.**

   - Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com)>`.
   - Aceite os avisos de segurança.
   - Clique na barra de endereço que exibe o erro de certificado.
   - Visualize o certificado.

3. Importe o certificado para o armazenamento de certificados em cada um dos seus Controllers.

   a. Clique na opção **Instalar certificado**, selecione **Máquina Local** e, em seguida, clique em **Avançar**.

b. Selecione **Colocar todos os certificados no seguinte armazenamento** e, em seguida, clique em **Procurar**. Selecione **Pessoas Confiáveis** e, em seguida, clique em **OK**. Clique em **Avançar** e, em seguida, clique em **Concluir**.

Se você alterar o nome do servidor vSphere após a instalação, deverá gerar um novo certificado autoassinado nesse servidor antes de importar o novo certificado.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do VMware, consulte Criar um catálogo VMware

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

## Conexão com a nuvem VMware e soluções de parceiros

Após configurar cluster da Solução VMware do Azure (AVS), Google Cloud VMware Engine e VMware Cloud on AWS, crie as conexões. Consulte Conexão com VMware para criar conexões.

### Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do VMware, consulte Criar um catálogo VMware

### Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

# Gerenciamento de imagens

## Introdução

O processo de criação ou atualização do catálogo MCS tem duas fases:

- Masterização: uma imagem de origem é convertida em uma imagem publicada
- Clonagem: novas VMs são criadas a partir da imagem publicada

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

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

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

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

> **Observação:**
>
> - Este recurso é atualmente aplicável a ambientes de virtualização Azure e VMware.
> - Você pode criar um catálogo de máquinas MCS sem usar imagens preparadas. Nesse caso, você não poderá obter os benefícios do recurso.
> - O recurso está geralmente disponível a partir do Citrix Virtual Apps and Desktops™ 2402 LTSR CU2.

## Casos de uso

Alguns dos casos de uso da funcionalidade de gerenciamento de imagens são:

- *Gerenciamento de versões*: As versões de imagem permitem que você:
  - gerenciar diferentes iterações ou atualizações de uma imagem específica.
  - manter várias versões de uma imagem para diferentes propósitos.
- *Agrupamento lógico*: Você pode criar várias definições de imagem para:
  - agrupar logicamente versões de imagem com base em vários critérios, como projeto, departamento ou tipo de aplicativo e desktop.
  - gerenciar imagens de forma mais eficiente dentro de uma organização.

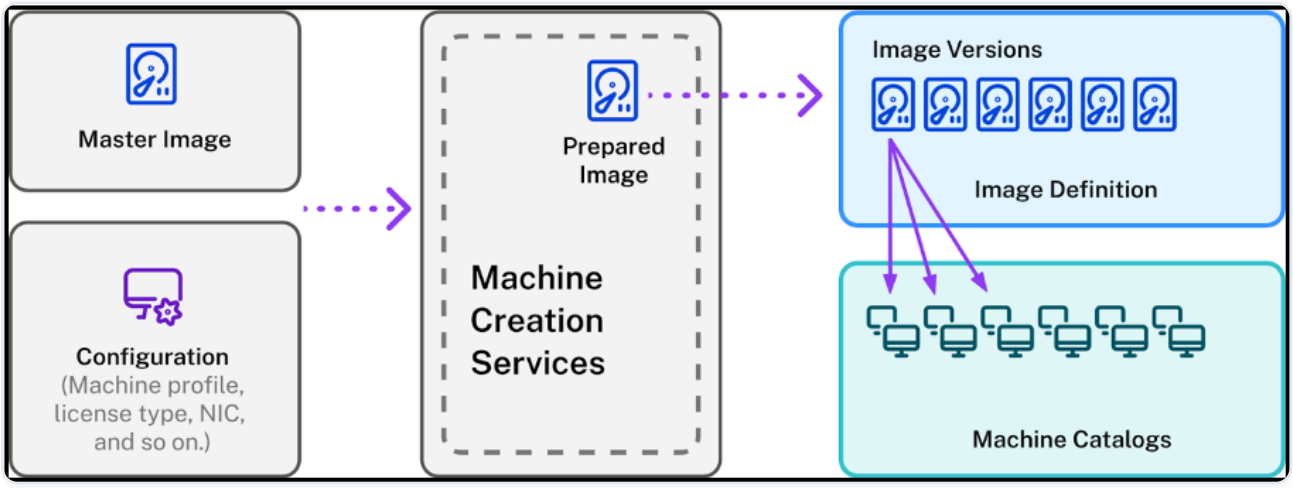
## O que é uma imagem preparada?

Com a funcionalidade de gerenciamento de imagens, o MCS desvincula a fase de masterização do fluxo de trabalho geral de criação ou atualização de catálogo e divide o processo em duas etapas:

1. Criar imagens preparadas a partir de uma única imagem de origem.
2. Usar a imagem preparada para criar ou atualizar um catálogo de máquinas MCS.

Você pode criar as imagens preparadas com antecedência. Você pode usar uma única imagem preparada para criar ou atualizar vários catálogos de máquinas provisionados pelo MCS.

Entenda como uma imagem preparada é usada em vários catálogos de máquinas MCS ao usar o Web Studio a partir da imagem:




*Definição de imagem*: As definições de imagem são um agrupamento lógico de versões de uma imagem. A definição de imagem contém informações sobre:

- por que a imagem foi criada
- para qual SO ela se destina
- outras informações sobre o uso da imagem.

Um catálogo não é criado a partir de uma definição de imagem, mas a partir das versões de imagem que são criadas com base na definição de imagem.

*Versão da imagem*: As versões da imagem gerenciam o versionamento para a definição da imagem. Uma definição de imagem pode ter várias versões de imagem. Use as versões da imagem como imagens preparadas para criar ou atualizar um catálogo.

Alternativamente, se você quiser usar comandos PowerShell para criar um esquema de provisionamento para criar ou atualizar um catálogo, então você deve criar uma especificação de

versão de imagem preparada com base na especificação de versão de imagem mestre, conforme necessário para o seu ambiente.

## Requisito

- Para imagens mestre do Windows, apenas imagens VDA versão 2311 ou posterior são suportadas. O componente MCS/IO deve ser explicitamente selecionado e instalado. A ativação ou desativação da configuração de E/S do MCS deve ser determinada durante a criação ou atualização do catálogo de máquinas, pois não está ativada por padrão.

## Limitações

Atualmente, o recurso não oferece suporte ao seguinte:

- Múltiplas NICs no Azure
- Recurso de disco de dados persistente
- Hibernação para multi-sessão
- Alteração do tipo de imagem

## Gerenciamento do ciclo de vida da imagem usando o Web Studio

O ciclo de vida da imagem ao usar o Web Studio é:

1. Criar uma imagem preparada: Crie uma definição de imagem e sua versão inicial.
2. Crie versões de imagem a partir da versão inicial da imagem.
3. Use uma versão de imagem como imagem preparada para criar catálogos.
4. Atualize um catálogo de máquinas com uma imagem preparada diferente.
5. Gerenciar as definições e versões de imagem: Editar o nome e a descrição das versões de imagem e a descrição de uma definição de imagem.
6. Excluir uma versão de imagem.
7. Excluir uma definição de imagem.

Alternativamente, você também pode gerenciar imagens usando o PowerShell. Consulte Gerenciamento do ciclo de vida da imagem usando o PowerShell.

## Criar ou atualizar um catálogo usando uma imagem preparada

Crie imagens preparadas e use as imagens preparadas para criar ou atualizar um catálogo de máquinas MCS usando:

- O Web Studio
- Os comandos do PowerShell

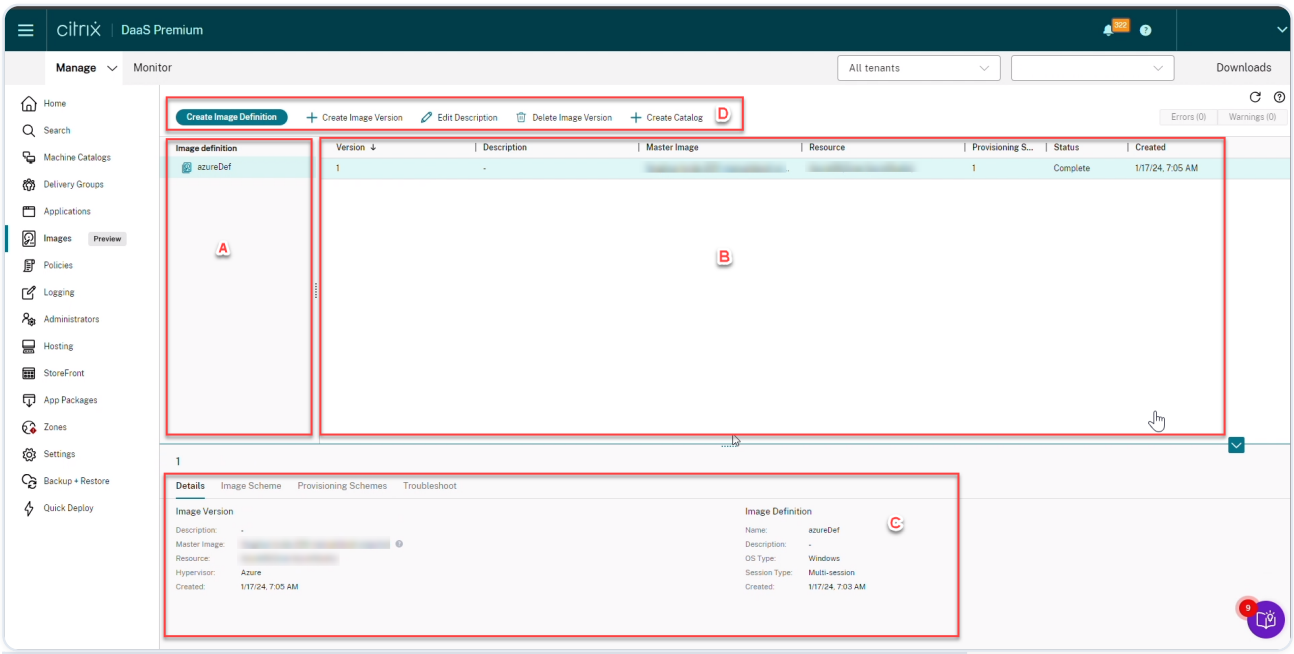
## Usar o Web Studio

Consulte os seguintes tópicos:

- Entender o nó Imagens
- Criar uma definição de imagem e versão inicial da imagem
- Criar versões de imagem
- Criar um catálogo de máquinas a partir do nó Imagens
- Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas
- Atualizar um catálogo de máquinas com uma imagem preparada diferente
- Gerenciar as definições e versões de imagem

### Compreender o nó Imagens

Use o nó **Imagens** para criar e gerenciar imagens preparadas por MCS. Sua visualização principal é dividida em quatro partes:




| RÓTULO | PARTE | DESCRIÇÃO |
| --- | --- | --- |
| A | Definições de imagem | Lista as definições de imagem criadas anteriormente. |

| RÓTULO | PARTE | DESCRIÇÃO |
|---|---|---|
| B | Versões de imagem | Exibe as versões de imagem da definição de imagem selecionada. |
| C | Detalhes | • A guia **Detalhes** exibe informações detalhadas sobre a definição ou versão de imagem selecionada, como Imagem Mestra, Recurso, Hypervisor, nome da definição de imagem, tipo de SO e tipo de sessão.<br>• A guia **Esquema de Imagem** exibe informações sobre o modelo usado para preparar imagens, como disco rígido, tamanho da máquina, tipo de licença, |

| RÓTULO | PARTE | DESCRIÇÃO |
| --- | --- | --- |
| | | conjunto de criptografia de disco, perfil da máquina e assim por diante.<br>• A guia **Esquemas de Provisionamento** exibe o nome do esquema de provisionamento usado para criar o catálogo.<br>• A guia **Solução de Problemas** fornece o status de erro da versão de imagem selecionada. |
| D | Barra de ações | Lista as ações que você pode realizar em definições e versões de imagem, como **Criar Versão da Imagem**, **Editar Descrição**, **Excluir Versão da Imagem** e **Criar Catálogo**. |

### Criar um catálogo de máquinas usando a imagem preparada

As principais etapas para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.

2. Use a versão da imagem como uma imagem preparada para criar um catálogo.

### Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. Faça login no Web Studio e selecione o nó **Imagens**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição da imagem.
3. Na página **Imagem**, selecione **Recursos** e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

   > **Observação:**
   >
   > Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. (Somente para Azure) Na página **Tipos de Armazenamento e Licenças**, selecione o tipo de armazenamento e licença a ser usado como parte do processo de preparação da imagem.

   > **Observação:**
   >
   > Se você selecionar um perfil de máquina na página **Imagem**, o tipo de licença do perfil de máquina será pré-selecionado com base na configuração do perfil.

5. Na página **Especificação da Máquina**:

   - Para Azure, selecione um tamanho de máquina. Se você selecionar um perfil de máquina na página **Imagem**, o tamanho da máquina do perfil de máquina será selecionado por padrão.
   - Para VMware, se você selecionar um perfil de máquina, poderá ver a contagem de CPUs Virtuais derivada do perfil de máquina e ela será inalterável. Se você não selecionar um perfil de máquina, poderá ver apenas o tamanho da memória derivado da imagem mestre.

6. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada.

   Para VMware, se você não selecionar um perfil de máquina, a NIC associada à imagem mestre será selecionada por padrão. Se você selecionar um perfil de máquina, as NICs serão derivadas do perfil de máquina e a contagem será inalterável.

   > **Observação:**
   >
   > Múltiplas NICs não são suportadas no Azure.

7. (Somente para Azure) Na página **Configurações de Disco**, selecione a chave de criptografia gerenciada pelo cliente (CMEK). Se o perfil da máquina não tiver uma CMEK, mas a imagem mestre tiver, ele pré-selecionará a CMEK da imagem mestre.
8. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
9. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

### Criar versões de imagem

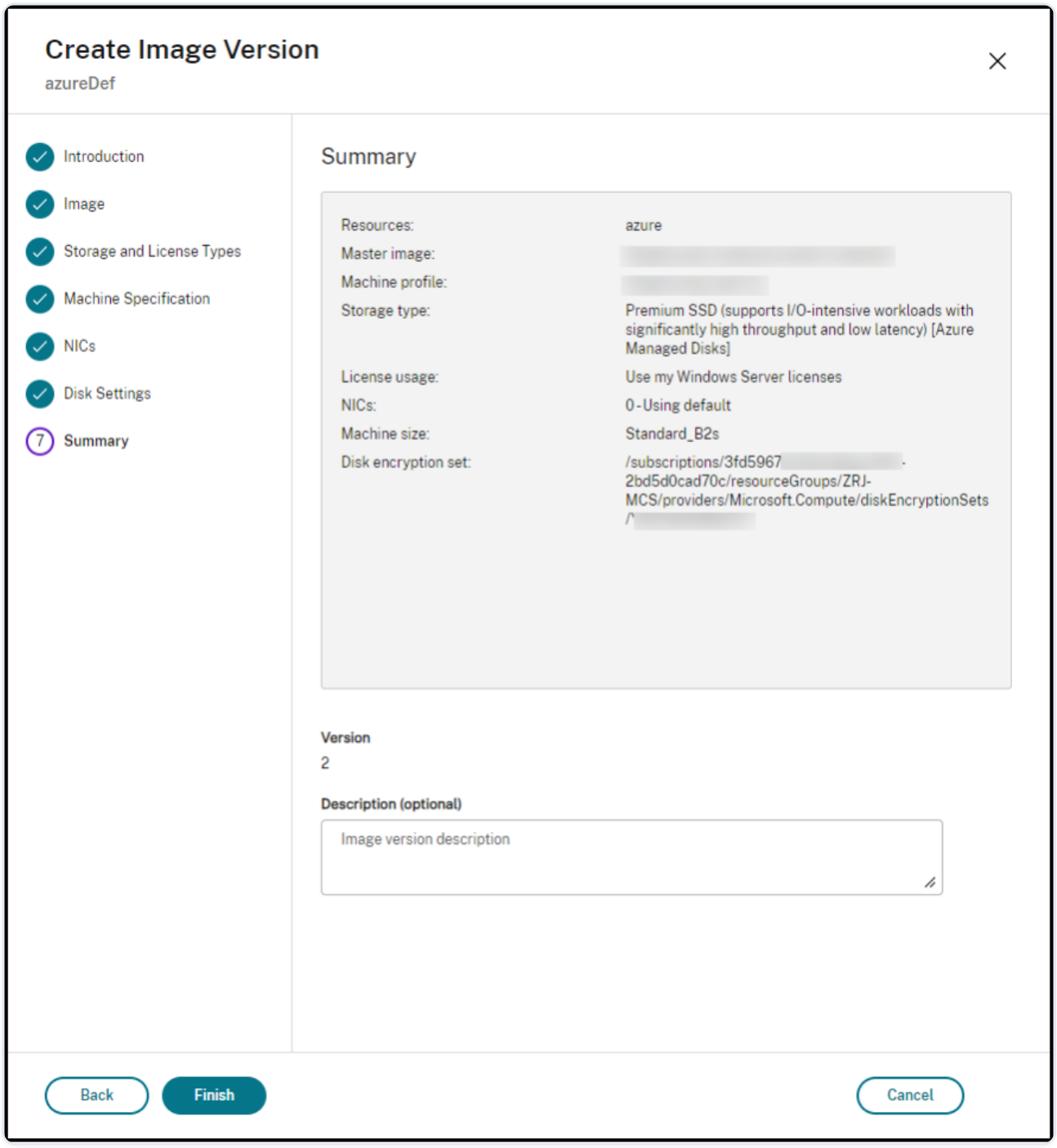
As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Observação:**
>
> A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá para o nó **Imagens**, selecione uma versão da imagem e selecione **Criar Versão da Imagem**.
2. Se você quiser que a configuração da versão da imagem seja diferente da versão da imagem configurada inicialmente, configure as definições nas páginas **Imagem**, **Tipos de Armazenamento e Licença**, **Especificação da Máquina**, **NICs** e **Configurações de Disco** da caixa de diálogo **Criar Versão da Imagem**.

3. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.




### Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho necessária.
3. Da página **Imagem** à página **Configurações de Disco**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. (Para Azure) Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
5. Conclua as configurações nas páginas seguintes.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
7. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

### Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de Máquina** e **Gerenciamento de Máquinas**.
3. Na página **Imagem**:
    a. Selecione **Imagem preparada**.
    b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem.
    c. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
    d. Se a versão da imagem selecionada estiver configurada com um perfil de máquina, selecione um perfil de máquina. Se a versão da imagem selecionada não estiver configurada com um perfil de máquina, você não poderá optar por usar um perfil de máquina.
4. Configure as configurações nas páginas a seguir.
5. Na página **Configurações de Disco**, se a imagem preparada selecionada usar um conjunto de criptografia de disco, você não poderá remover o conjunto de criptografia, mas poderá alterar a chave para outra chave de criptografia.

6. (Para Azure) Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
7. Conclua as configurações nas páginas seguintes.
8. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

### Atualizar um catálogo de máquinas com uma imagem preparada diferente

Para atualizar um catálogo de máquinas MCS existente com uma imagem preparada diferente, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo e selecione um catálogo de máquinas que você deseja atualizar. Clique com o botão direito e selecione **Alterar Imagem Preparada**.
2. Na página **Imagem**, selecione uma imagem preparada.
3. Na página **Estratégia de implantação**, selecione quando você deseja atualizar este catálogo com a imagem preparada selecionada.
4. Na página **Resumo**, verifique os detalhes. Clique em **Concluir**.

**Você pode ver o histórico de alterações de imagem feitas em um catálogo. Para ver o histórico, faça o seguinte:**

1. Selecione um catálogo de máquinas.
2. Na guia **Propriedades do Modelo**, no campo **Imagem preparada**, clique em **Exibir histórico da imagem**.

### Gerenciar as definições e versões de imagem

Você pode editar e excluir as definições e versões de imagem para gerenciar o uso de várias versões e definições de imagem criadas.

#### Editar uma definição de imagem

Você pode editar o nome e a descrição de uma definição de imagem.

Para editar uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Editar Definição de Imagem**.

### Editar versão da imagem

Você pode editar a descrição de uma versão 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 de 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 de imagem e selecione **Excluir Versão da Imagem**.

> **Nota:**
>
> Você não pode excluir uma versão de imagem se ela for usada por um catálogo de máquinas.

### Excluir uma definição de imagem

Para excluir uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Excluir Definição de Imagem**.

> **Nota:**
>
> Não é possível excluir uma definição de imagem se ela contiver uma versão de imagem.

### Gerenciamento do ciclo de vida da imagem usando PowerShell

Se você quiser usar comandos do PowerShell para criar um esquema de provisionamento, deverá criar uma especificação de versão de imagem preparada com base na especificação de versão de imagem mestre, conforme necessário para seu ambiente.

*Especificação de versão da imagem mestre*: Uma especificação de versão da imagem mestre é uma imagem específica adicionada ou criada em uma versão de imagem. Você pode adicionar uma imagem existente no hipervisor como uma especificação de versão da imagem mestre ou criar uma especificação de versão da imagem preparada com base na especificação da imagem

mestre, conforme necessário para seu ambiente. A especificação de versão da imagem preparada pode ser usada para vários esquemas de provisionamento.

O ciclo de vida de uma imagem ao usar comandos do PowerShell é:

1. Criar uma imagem:
    a. Criar uma definição de imagem.
    b. Criar uma versão de imagem.
    c. Adicionar uma especificação de versão de imagem mestre.
    d. Criar uma especificação de versão de imagem preparada.
2. Criar um catálogo de máquinas MCS usando uma especificação de versão de imagem preparada:
    a. Criar um catálogo de broker.
    b. Crie um pool de identidades.
    c. Criar um esquema de provisionamento com o parâmetro Uid da especificação de versão de imagem preparada usando o comando `New-ProvScheme`.
    d. Vincular o catálogo de broker ao esquema de provisionamento.
3. Criar VMs no catálogo de máquinas MCS.
4. Alterar a especificação de versão de imagem preparada de um esquema de provisionamento usando o comando `Set-ProvScheme`.
5. Gerenciar as definições e versões de imagem: Editar as versões de imagem e as definições de imagem.
6. Excluir um catálogo de máquinas MCS: A ordem de exclusão é: especificação de versão de imagem preparada > especificação de versão de imagem mestre > versão de imagem > definição de imagem. Antes de excluir a especificação de versão de imagem, certifique-se de que a especificação de versão de imagem preparada não esteja associada a nenhum catálogo de máquinas MCS.

## Usar o PowerShell

Você pode fazer o seguinte usando comandos PowerShell:

- Criar uma imagem preparada
- Criar um catálogo usando a especificação de versão de imagem preparada

- Atualizar um catálogo usando uma especificação de versão de imagem preparada(#update-a-catalog-using-a-prepared-image-version-spec)
- Excluir definição de imagem, versão de imagem e especificação de versão de imagem preparada(#delete-image-definition-image-version-and-prepared-image-version-spec)
- Gerenciar definição de imagem e versão de imagem(#manage-image-definition-and-image-version)
- Obter definição de imagem, versão de imagem, especificação de versão de imagem preparada e detalhes do esquema de provisionamento(#get-image-definition-image-version-prepared-image-version-spec-and-provisioning-scheme-details)

### Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação da versão da imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

   ```
   New-ProvImageVersion -ImageDefinitionName image1 -Description "version
   1"
   ```

4. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

   ```
   Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
   ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
   ```

```
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

**Nota:**

Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

5. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"

-ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

**Nota:**

Uma unidade de hospedagem e tipo de preparação podem ter apenas uma instância preparada.

**Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada no Azure**:

```
$ImageDefintion = New-ProvImageDefinition

-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
```

```
MultiSession

 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win2022-
snapshot.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName azure -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"} -ServiceOffering
"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"></CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

**Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada no VMware:**

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2
-OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware -MasterImagePath
$MasterImagePath
```

```
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

**Nota:**

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.
- Não é possível especificar um grupo de recursos ao criar uma especificação de versão de imagem.

### Criar um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

**Exemplo do conjunto completo de comandos Powershell para criar um catálogo no Azure:**

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /></
CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
```

```
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

**Exemplo do conjunto completo de comandos Powershell para criar um catálogo no VMware:**

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

### Atualizar um catálogo usando uma especificação de versão de imagem preparada

Você pode atualizar um catálogo usando o comando `Set-ProvSchemeImage`. Por exemplo,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

Ou,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

**Exemplo do conjunto completo de comandos Powershell para atualizar um catálogo:**

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"

Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

### Excluir definição de imagem, versão de imagem e especificação de versão de imagem preparada

Considere o seguinte antes de excluir uma definição de imagem, versão de imagem e especificação de versão de imagem preparada:

- Uma definição de imagem não pode ser excluída se contiver qualquer versão de imagem.
- Uma versão de imagem não pode ser excluída se contiver qualquer especificação de versão de imagem.
- Uma especificação de versão de imagem mestre não pode ser excluída se for usada por qualquer outra especificação de versão de imagem preparada.
- Uma especificação de versão de imagem preparada não pode ser excluída se estiver sendo usada por qualquer esquema de provisionamento.

Os passos detalhados são os seguintes:

1. Remover uma especificação de versão de imagem preparada. Por exemplo,

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec
   -ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
   "PreparationType -eq 'Mcs'"

   Remove-ProvImageVersionSpec -ImageVersionSpecUid
   $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
   ```

   **Nota:**

> A especificação de versão de imagem mestre só pode ser excluída quando não houver nenhuma especificação de versão de imagem preparada associada.

2. Remover especificação de versão de imagem mestre. Por exemplo,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

3. Remover uma versão de imagem. Por exemplo,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

4. Remover uma definição de imagem. Por exemplo,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos PowerShell:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1

Remove-ProvImageDefinition -ImageDefinitionName image1
```

### Gerenciar definição de imagem e versão de imagem

Você pode renomear e editar uma definição de imagem, e editar uma versão de imagem.

- Renomear uma definição de imagem usando o comando `Rename-ProvImageDefinition`. Por exemplo:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  Ou,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- Editar uma definição de imagem usando o comando `Set-ProvImageDefinition`. Por exemplo:

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

  Ou,

  ```
  Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
  <string>]
  ```

- Editar uma versão de imagem usando o comando `Set-ProvImageVersion`. Por exemplo:

  ```
  Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
  ```

  Ou,

  ```
  Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
  <int> [-Description <string>]
  ```

### Obter detalhes de definição de imagem, versão de imagem, especificação de versão de imagem preparada e esquema de provisionamento

- Obtenha detalhes da definição da imagem usando o comando `Get-ProvImageDefinition`. Por exemplo:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- Obtenha detalhes da versão da imagem usando o comando `Get-ProvImageVersion`. Por exemplo:
  - Para listar as versões da imagem em uma definição de imagem,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Para obter um detalhe da versão da imagem,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    -ImageVersionNumber <int>
    ```

- Obtenha a especificação da versão da imagem preparada usando o comando `Get-ProvImageVersionSpec`. Por exemplo:
  - Para listar todas as especificações de versão de imagem preparada em uma versão de imagem,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

- Para listar as especificações da versão da imagem mestre em uma especificação da versão da imagem preparada,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

- Para listar as especificações da versão da imagem preparada em uma versão da imagem, que está associada a uma imagem mestre,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

- Para obter especificações de versão de imagem preparada bem-sucedidas em uma versão de imagem,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

- Para obter um detalhe da especificação da versão da imagem preparada,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Obtenha os detalhes do esquema de provisionamento usando o comando `Get-ProvScheme`. Por exemplo:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- Obtenha o histórico da especificação da versão da imagem preparada de um esquema de provisionamento usando o comando `Get-ProvSchemeImageVersionSpecHistory`. Por exemplo:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

# Criar catálogos de máquinas

**Importante:**

A partir do Citrix Virtual Apps and Desktops™ 7 2006, se sua implantação atual usar alguma das seguintes tecnologias, você poderá atualizar sua implantação para a versão atual somente após remover os itens de Fim de Vida (EOL) que usam essas tecnologias.

- vDisks Pessoais (PvDs)
- AppDisks™
- Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic

Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

**Nota:**

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

Se você deseja usar conexões de host de nuvem pública para sua implantação, você precisa de uma Licença de Direitos Híbridos para concluir sua nova instalação ou atualização para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização pausa ou para. Uma mensagem explicativa

aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

## Introdução

Coleções de máquinas físicas ou virtuais são gerenciadas como uma única entidade chamada catálogo de máquinas. Todas as máquinas em um catálogo têm o mesmo tipo de sistema operacional: SO multi-sessão ou SO de sessão única, e máquinas Windows ou Linux.

O Web Studio o guia para criar o primeiro catálogo de máquinas depois de criar o site. Depois de criar o primeiro catálogo, o Web Studio o guia para criar o primeiro grupo de entrega. Mais tarde, você pode alterar o catálogo que criou e criar mais catálogos.

> **Dica:**
>
> A atualização de uma implantação existente habilita o recurso de otimização de armazenamento do Machine Creation Services (MCS) (MCS I/O), nenhuma configuração adicional é necessária. A atualização do Virtual Delivery Agent (VDA) e do Delivery Controller manipular a atualização do MCS I/O.

## Visão geral

Ao criar um catálogo de VMs, você especifica como provisionar essas VMs. Você pode usar o Machine Creation Services™ (MCS). Ou, você pode usar suas próprias ferramentas para fornecer máquinas.

Considere:

- O MCS suporta um único disco de sistema da imagem da máquina virtual. Ele ignora o restante dos discos de dados anexados a essa imagem.
- Se você usa o MCS para provisionar VMs, você fornece uma imagem mestre (ou snapshot de uma imagem) para criar VMs idênticas no catálogo. Antes de criar o catálogo, você primeiro usa as ferramentas para criar e configurar a imagem mestre. Este processo inclui a instalação de um Virtual Delivery Agent (VDA) na imagem. Em seguida, você cria o catálogo de máquinas no Web Studio. Você seleciona essa imagem (ou snapshot), especifica o número de VMs a serem criadas no catálogo e configura informações adicionais.
- Se suas máquinas já estiverem disponíveis, você ainda deve criar um ou mais catálogos de máquinas para essas máquinas.

- Se você estiver criando um catálogo usando o PowerShell SDK diretamente, poderá especificar um modelo de hipervisor (**VMTemplates**), em vez de uma imagem ou um instantâneo.
- O uso de um modelo para provisionar um catálogo é considerado um recurso experimental. Ao usar este método, a preparação da máquina virtual pode falhar. Como resultado, o catálogo não pode ser publicado usando o modelo.

Ao usar o MCS ou o Citrix Provisioning™ para criar o primeiro catálogo, você usa a conexão de host que configurou ao criar o site. Mais tarde (depois de criar seu primeiro catálogo e grupo de entrega), você pode alterar informações sobre essa conexão ou criar mais conexões.

Depois de concluir o assistente de criação de catálogo, os testes são executados automaticamente para garantir que ele esteja configurado corretamente. Quando os testes forem concluídos, você poderá visualizar um relatório de teste. Execute os testes a qualquer momento no Web Studio.

> **Observação:**
>
> O MCS não oferece suporte ao Windows 10 IoT Core e ao Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

> Para obter detalhes técnicos sobre as ferramentas do Citrix Provisioning, consulte Gerenciamento de Imagens do Citrix Virtual Apps and Desktops.

### Verificação de licença RDS

Atualmente, o Web Studio não executa a verificação de licenças RDS da Microsoft válidas ao criar um catálogo de máquinas que contém máquinas de SO Windows multi-sessão. Para visualizar o status da licença RDS da Microsoft para uma **máquina de SO multi-sessão** do Windows, vá para o Citrix Director. Visualize o status da licença RDS da Microsoft no painel **Detalhes da Máquina**. Este painel está na página **Detalhes da Máquina e Detalhes do Usuário**. Para obter mais informações, consulte Integridade da licença RDS da Microsoft.

### Registro de VDA

Um VDA deve ser registrado em um Delivery Controller™ ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos que, de outra forma, estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador pode solucionar. O Web Studio fornece informações de solução de

problemas no assistente de criação de catálogo e depois que você adiciona máquinas de um catálogo a um grupo de entrega.

Depois de adicionar máquinas existentes usando o assistente, a lista de nomes de contas de computador indica se cada máquina é adequada para ser adicionada ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre essa máquina.

Se a mensagem identificar uma máquina problemática, remova essa máquina ou adicione-a. Por exemplo, se uma mensagem indicar que as informações podem não ser obtidas sobre uma máquina, adicione a máquina de qualquer maneira.

Para mais informações, consulte:

- CTX136668 para orientação sobre solução de problemas de registro de VDA
- Versões de VDA e níveis funcionais
- Métodos de registro de VDA

### Resumo da criação de catálogo MCS

Aqui está uma breve visão geral das ações padrão do MCS depois que você fornece informações no assistente de criação de catálogo.

- Se você selecionou uma imagem mestre (em vez de um instantâneo), o MCS cria um instantâneo.
- O MCS cria uma cópia completa do snapshot e a coloca em cada local de armazenamento definido na conexão do host.
- O MCS adiciona as máquinas ao Active Directory, o que cria identidades exclusivas.
- O MCS cria o número de VMs especificado no assistente, com dois discos definidos para cada VM. Além dos dois discos por VM, um mestre também é armazenado no mesmo local de armazenamento. Se você tiver vários locais de armazenamento definidos, cada um receberá os seguintes tipos de disco:
    - A cópia completa do instantâneo que é somente leitura e compartilhada entre as VMs recém-criadas.
    - Um disco de identidade exclusivo de 16 MB que dá a cada VM uma identidade única. Cada VM recebe um disco de identidade.
    - Um disco de diferença exclusivo para armazenar gravações feitas na VM. Este disco é provisionado de forma dinâmica (se suportado pelo armazenamento do host) e aumenta

para o tamanho máximo da imagem mestre, se necessário. Cada VM recebe um disco de diferença. O disco de diferença retém as alterações feitas durante as sessões. É permanente para desktops dedicados. Para desktops agrupados, ele é excluído e um novo é criado após cada reinício via o controlador de entrega.

Alternativamente, ao criar VMs para entregar desktops estáticos, você pode especificar (na página **Máquinas** do assistente de criação de catálogo) clones de VM espessos (cópia completa). Clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem seu próprio arquivo.

### Considerações de armazenamento do MCS

Existem muitos fatores ao decidir sobre soluções de armazenamento, configurações e capacidades para o MCS. As informações a seguir fornecem considerações adequadas para a capacidade de armazenamento:

*Considerações de capacidade:*

- Discos

  Os discos Delta ou de Diferença (Diff) consomem a maior quantidade de espaço na maioria das implantações do MCS para cada VM. Cada VM criada pelo MCS recebe no mínimo 2 discos na criação.

  - Disk0 = Disco de Diferença: contém o SO quando copiado da Imagem Base Mestra.
  - Disk1 = Disco de Identidade: 16 MB - contém dados do Active Directory para cada VM.

  À medida que o produto evolui, pode ser necessário adicionar mais discos para satisfazer certos casos de uso e consumo de recursos. Por exemplo:

  - Otimização de Armazenamento MCS cria um disco estilo cache de gravação para cada VM.
  - O MCS adicionou a capacidade de usar clones completos em oposição ao cenário de disco Delta descrito na seção anterior.

  Recursos do hipervisor também podem entrar na equação. Por exemplo:

  - XenServer IntelliCache cria um Disco de Leitura no armazenamento local para cada XenServer. Esta opção economiza IOPS em relação à imagem mestre que pode estar localizada no armazenamento compartilhado.

- Sobrecarga do hypervisor

Diferentes hypervisors usam arquivos específicos que criam sobrecarga para VMs. Os hypervisors também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir a sobrecarga para:

- Arquivos de log
- Arquivos específicos do hypervisor. Por exemplo:
  - O VMware adiciona mais arquivos à pasta **VM storage**. Consulte Melhores Práticas do VMware.
  - Calcule os requisitos totais de tamanho da sua máquina virtual. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de troca e 100 MB para arquivos de log, consumindo um total de 36,1 GB.
- Snapshots para XenServer; Snapshots para VMware.

- Sobrecarga do processo

  A criação de um catálogo, a adição de uma máquina e a atualização de um catálogo têm implicações de armazenamento únicas. Por exemplo:

  - Criação inicial do catálogo requer que uma cópia do disco base seja copiada para cada local de armazenamento.
    - Também exige que você crie uma VM de Preparação temporariamente.
  - Adicionar uma máquina a um catálogo não requer a cópia do disco base para cada local de armazenamento. A criação do catálogo varia com base nos recursos selecionados.
  - Atualizar o catálogo para criar um disco base extra em cada local de armazenamento. As atualizações do catálogo também experimentam um pico temporário de armazenamento onde cada VM no catálogo tem 2 discos Diff por um certo período de tempo.

*Mais considerações:*

- **Dimensionamento da RAM:** Afeta o tamanho de certos arquivos e discos do hypervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de snapshot.
- **Thin / Thick provisioning:** O armazenamento NFS é preferido devido aos recursos de provisionamento thin.

### Otimização de armazenamento do Machine Creation Services (MCS)

Com o recurso de otimização de armazenamento do Machine Creation Services (MCS), referido como MCS I/O:

- O contêiner de cache de gravação é *baseado em arquivo*, a mesma funcionalidade encontrada no Citrix Provisioning. Por exemplo, o nome do arquivo de cache de gravação do Citrix Provisioning é `D:\vdiskdif.vhdx` e o nome do arquivo de cache de gravação do MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico incluindo suporte para um arquivo de despejo de memória (crash dump) do Windows gravado no disco de cache de gravação.
- O MCS I/O mantém a tecnologia *cache na RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação de várias camadas mais otimizada. Essa funcionalidade permite que um administrador equilibre o custo em cada camada, RAM e disco, e o desempenho para atender à expectativa de carga de trabalho desejada.

A atualização do método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. O MCS I/O não suporta mais cache somente RAM. Especifique um tamanho de disco no Web Studio durante a criação do catálogo de máquinas.
2. O disco de cache de gravação da VM é criado e formatado automaticamente ao inicializar uma VM pela primeira vez. Assim que a VM estiver ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.
3. O arquivo de paginação é redirecionado para este volume formatado, `MCSWCDisk`. Como resultado, esse tamanho de disco considera a quantidade total de espaço em disco. Ele inclui o delta entre o tamanho do disco e a carga de trabalho gerada mais o tamanho do arquivo de paginação. Isso geralmente está associado ao tamanho da RAM da VM.

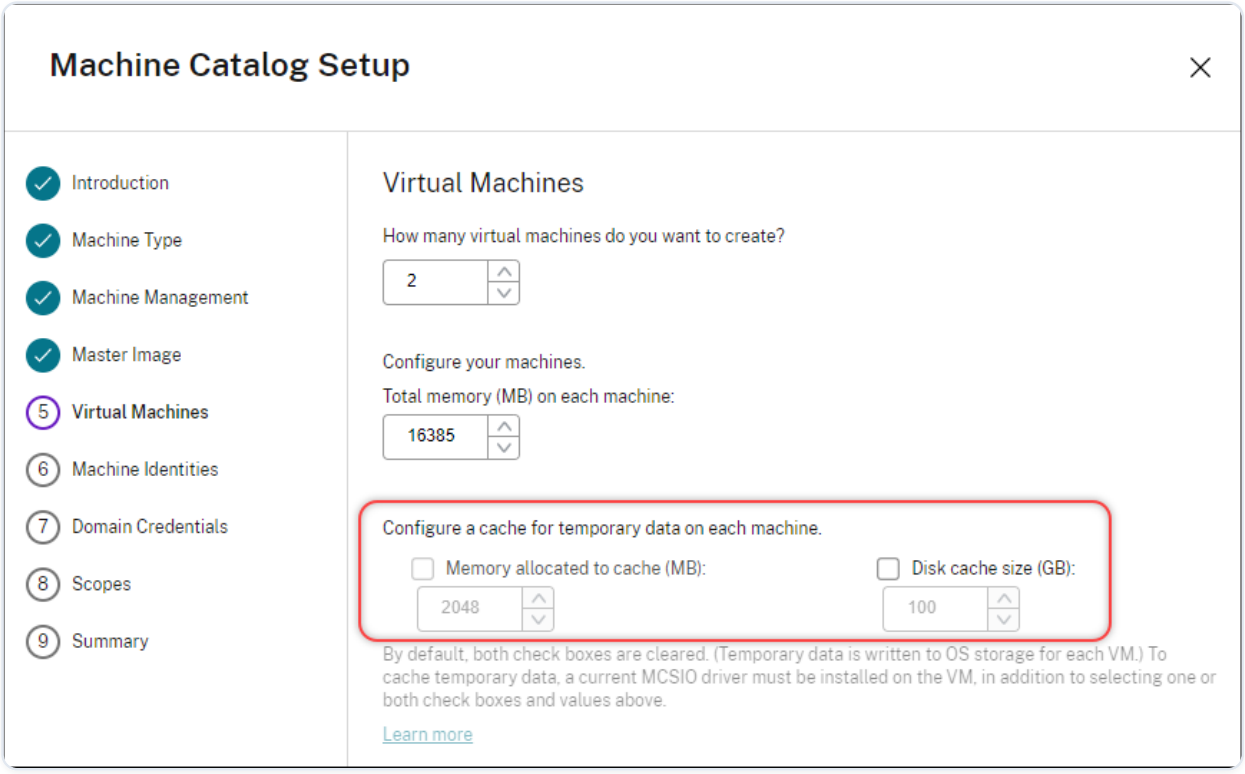
### Habilitando atualizações de otimização de armazenamento MCS

Para habilitar a funcionalidade de otimização de armazenamento do MCS I/O, atualize o Delivery Controller e o VDA para a versão mais recente do Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será necessária. A atualização do VDA e do Delivery Controller manipular a atualização do MCS I/O.

> Ao habilitar a atualização de otimização de armazenamento do MCS, considere o seguinte:

- Ao criar um catálogo de máquinas, o administrador pode configurar o tamanho da RAM e do disco.




- A atualização de um catálogo de máquinas existente para um novo snapshot de VM contendo um VDA configurado para a versão 1903 resulta no seguinte comportamento: o novo snapshot continua a usar a configuração de E/S do MCS do catálogo existente para RAM e tamanho do disco. O disco bruto existente é formatado.

**Importante:**

A otimização de armazenamento do MCS mudou com a versão 1903 do Citrix Virtual Apps and Desktops. Esta versão suporta a tecnologia de cache de gravação baseada em arquivo, proporcionando melhor desempenho e estabilidade. A nova funcionalidade fornecida pelo MCS I/O pode exigir um requisito de armazenamento de cache de gravação maior em comparação com as versões anteriores do Citrix Virtual Apps and Desktops. A Citrix recomenda que você reavalie o tamanho do disco para garantir que ele tenha espaço em disco suficiente para o fluxo de trabalho alocado e um tamanho de arquivo de paginação extra. O tamanho do arquivo de paginação geralmente está relacionado à quantidade de RAM do sistema. Se o tamanho do disco do catálogo existente for insuficiente, crie um catálogo de máquinas e aloque um disco de cache de gravação maior.

# Atribuir uma letra de unidade específica ao disco de cache de gravação de E/S do MCS

Você pode atribuir uma letra de unidade específica ao disco de cache de gravação de E/S do MCS. Essa implementação ajuda a evitar conflitos entre a letra de unidade de quaisquer aplicativos que você usa e a letra de unidade do disco de cache de gravação de E/S do MCS. Para atribuir uma letra de unidade ao disco de cache de gravação de E/S do MCS, você pode usar comandos do PowerShell. Os hipervisores suportados são Azure, GCP, VMware, SCVMM e XenServer.

> **Nota:**
>
> Este recurso requer a versão 2305 do VDA ou posterior.

## Limitações

- Aplicável apenas ao sistema operacional Windows
- Letra de unidade aplicável para disco de cache de write-back: `E` a `Z`
- Não aplicável quando o disco temporário do Azure é usado como disco de cache de write-back
- Aplicável somente ao criar um novo catálogo de máquinas

## Atribuir uma letra de unidade ao disco de cache de gravação

Para atribuir uma letra de unidade a um disco de cache de write-back:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades se ainda não tiver sido criado.
4. Crie um esquema de provisionamento usando o comando `New-ProvScheme` com a propriedade `WriteBackCacheDriveLetter`. Por exemplo:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `
```

```
-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
```

```
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. Conclua a criação do catálogo. 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 conexão, consulte Conexões e recursos.

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

É bom saber:

- Uma imagem mestre também pode ser conhecida como imagem de clone, imagem dourada, VM base ou imagem base. Os fornecedores de host usam termos diferentes.
- Certifique-se de que o host tenha processadores, memória e armazenamento suficientes para acomodar o número de máquinas criadas.
- Configure a quantidade correta de espaço em disco rígido necessário para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo de máquinas.
- Os catálogos de máquinas do Acesso Remoto para PC não usam imagens mestre.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou VMware tools). Se você omitir esta etapa, os aplicativos e desktops podem não funcionar corretamente.
- Um VDA. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.

- Ferramentas de terceiros conforme necessário, como software antivírus ou agentes de distribuição eletrônica de software. Configure os serviços com configurações apropriadas para os usuários e o tipo de máquina (como recursos de atualização).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda virtualizar aplicativos. A virtualização reduz custos, eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduzem o tamanho dos discos rígidos da imagem mestre, o que economiza custos de armazenamento.
- Clientes App-V com as configurações recomendadas, se você planeja publicar aplicativos App-V. O cliente App-V está disponível na Microsoft.
- Ao usar o MCS, se você localizar o Microsoft Windows, instale as localidades e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam as localidades e os pacotes de idiomas instalados.

**Importante:**

Se você estiver usando o MCS, não execute o Sysprep em imagens mestre.

Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e, em seguida, instale o sistema operacional, além de todos os service packs e atualizações. Especifique o número de vCPUs. Você também pode especificar o valor da vCPU se criar o catálogo de máquinas usando o PowerShell. Você não pode especificar o número de vCPUs ao criar um catálogo usando o Web Studio. Configure a quantidade de espaço em disco rígido necessária para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo.
2. Certifique-se de que o disco rígido esteja conectado no local do dispositivo 0. A maioria dos modelos de imagem mestre padrão configura este local por padrão, mas alguns modelos personalizados podem não fazê-lo.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, junte a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas. Se você estiver usando o MCS, não é necessário unir a

imagem mestre a um domínio. As máquinas provisionadas são unidas ao domínio especificado no assistente de criação de catálogo.

5. A Citrix recomenda que você crie e nomeie um snapshot da sua imagem mestre. Se você especificar uma imagem mestre em vez de um snapshot ao criar um catálogo, o Web Studio criará um snapshot. Você não pode nomeá-lo.

## Ativação de licenciamento por volume

O MCS oferece suporte à ativação de licenciamento por volume para automatizar e gerenciar a ativação de sistemas operacionais Windows e Microsoft Office. Os três modelos que o MCS oferece suporte para ativação de licenciamento por volume são:

- Serviço de Gerenciamento de Chaves (KMS)
- Ativação baseada no Active Directory (ADBA)
- Chave de Ativação Múltipla (MAK)

Você pode alterar a configuração de ativação depois de criar o catálogo de máquinas.

### Serviço de Gerenciamento de Chaves (KMS)

O KMS é um serviço leve que não requer um sistema dedicado e pode ser facilmente co-hospedado em um sistema que fornece outros serviços. Essa funcionalidade é suportada em todas as versões do Windows suportadas pela Citrix. Durante a preparação da imagem, o MCS realiza o rearm do KMS do Microsoft Windows e do Microsoft Office. Você pode pular o rearm executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre o Rearm do KMS do Microsoft Windows e do Microsoft Office durante a preparação da imagem, consulte Machine Creation Services: Visão geral da preparação da imagem e solução de problemas. 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 ativar máquinas por meio de suas conexões de domínio. As máquinas são ativadas imediatamente quando ingressam no domínio. Essas máquinas permanecem ativadas

enquanto permanecerem ingressadas no domínio e em contato com ele. Essa funcionalidade é suportada em todas as versões do Windows compatíveis com Citrix. Para obter mais informações sobre a ativação baseada no Active Directory, consulte Ativar usando ativação baseada no Active Directory.

### Chave de Ativação Múltipla (MAK)

MAK é uma forma de ativar o volume e autenticar o sistema Windows com a ajuda do servidor Microsoft. Você deve comprar a chave MAK da Microsoft, que é atribuída a um número fixo de contagens de ativação. Cada vez que um sistema Windows é ativado, a contagem de ativação é reduzida. Existem duas maneiras de ativar o sistema:

- Ativação Online: Se o sistema Windows que você deseja ativar tiver acesso à internet, o sistema ativa automaticamente o Windows ao instalar a chave do produto. Esse processo reduz a contagem de ativação em 1 para o MAK correspondente.
- Ativação Offline: Se o sistema Windows não conseguir se conectar à internet para fazer a ativação online, o MCS obtém um ID de confirmação e um ID de instalação do servidor Microsoft para ativar o sistema Windows. Essa forma de ativação é útil para catálogos de máquinas não persistentes.

> **Nota:**
>
> - O MCS não oferece suporte à ativação do Microsoft Office usando MAK.
> - A versão mínima do VDA necessária é 2303.

#### Requisitos principais

- O Delivery Controller deve ter acesso à internet.
- Crie um novo catálogo se a nova imagem a ser atualizada tiver uma Chave MAK diferente da original.
- Instale a chave MAK na imagem mestre. Consulte Implantar Ativação MAK para obter as etapas para instalar a Chave MAK em um Sistema Windows.
- Se você não estiver usando a preparação de imagem:

  a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

b. Defina o valor como `1`.

### Contagens de Ativação

Para visualizar o número de ativações restantes para a Chave MAK ou para verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação de Volume (VAMT). Consulte Instalar VAMT.

### Ativar o sistema Windows usando MAK

Para ativar o sistema Windows usando MAK:

1. Instale a chave do produto na imagem mestre. Esta etapa consome uma contagem de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagem:

   a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

   b. Defina o valor como `1`.

   Este método desabilita a opção de ativação online.
4. Adicione VMs ao catálogo de máquinas.
5. Ligar as VMs.
6. Dependendo se é ativação online ou offline, o sistema Windows é ativado.

   - Se a ativação for online, o sistema Windows é ativado após a instalação da chave do produto.
   - Se a ativação for offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. O MCS então recupera um ID de confirmação e um ID de instalação do servidor Microsoft. Esses IDs são usados para ativar o sistema Windows.

### Solução de problemas

Se a VM provisionada não for ativada com a chave MAK instalada, execute o comando `Get-ProvVM` ou `Get-ProvScheme` em uma janela do PowerShell.

- O comando `Get-ProvScheme`: Consulte o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS da imagem mestre mais recente.

- O comando `Get-ProvVM`. Consulte os parâmetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Você pode verificar o erro e as etapas para resolver o problema.

## Criar um catálogo de máquinas usando o Web Studio

Antes de criar um catálogo:

- Revise esta seção para saber mais sobre as escolhas que você faz e as informações que você fornece.
- Certifique-se de ter criado uma conexão com o hipervisor, serviço de nuvem e outros recursos que hospedam suas máquinas.
- Se você criou uma imagem mestre para provisionar máquinas, certifique-se de ter instalado um VDA nessa imagem.

Para iniciar o assistente de criação de catálogo:

1. Se este for o primeiro catálogo a ser criado, você será guiado para a seleção correta (como "Configurar as máquinas e criar catálogos de máquinas para executar aplicativos e desktops"). O assistente de criação de catálogo é aberto.
2. Se você já criou um catálogo e deseja criar outro, siga estas etapas:

    a. Faça login no Web Studio, selecione **Catálogos de Máquinas** no painel esquerdo e, em seguida, selecione **Criar Catálogo de Máquinas** na barra de ações.

    b. Para organizar catálogos usando pastas, crie pastas sob a pasta padrão **Catálogos de Máquinas**. Para obter mais informações, consulte Criar uma pasta de catálogo.

    c. Selecione a pasta onde você deseja criar o catálogo e clique em **Criar Catálogo de Máquinas**. O assistente de criação de catálogo é aberto.

O assistente o guiará pelos seguintes itens. As páginas do assistente que você vê diferem, dependendo das seleções que você faz.

## Sistema operacional

Cada catálogo contém máquinas de apenas um tipo. Selecione um.

- **SO multissessão:** Um catálogo de SO multissessão fornece desktops compartilhados hospedados. As máquinas podem estar executando versões compatíveis dos sistemas

operacionais Windows ou Linux, mas o catálogo não pode conter ambos. (Consulte a documentação do Linux VDA para obter detalhes sobre esse SO.)

- **SO de sessão única:** Um catálogo de SO de sessão única fornece desktops VDI que você pode atribuir a vários usuários diferentes.
- **Acesso Remoto a PC:** Um catálogo de Acesso Remoto a PC fornece aos usuários acesso remoto às suas máquinas de desktop físicas do escritório. O Acesso Remoto a PC não requer uma VPN para fornecer segurança.

## Gerenciamento de máquinas

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

A página **Gerenciamento de Máquinas** indica como as máquinas são gerenciadas e quais ferramentas você usa para implantar máquinas.

Escolha se as máquinas no catálogo são gerenciadas por energia através do Web Studio.

- As máquinas são gerenciadas em termos de energia através do Web Studio, por exemplo, VMs ou PCs blade. Esta opção está disponível somente se você já configurou uma conexão com um host.
- As máquinas não são gerenciadas em termos de energia através do Web Studio, por exemplo, máquinas físicas.

Se você indicou que as máquinas são gerenciadas por energia através do 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 imagem usando o MCS. O MCS copia imagens clonadas de uma imagem mestre para essas VMs.
  - **Citrix Provisioning Services (PVS)** Cria um catálogo de VMs provisionadas usando MCS e com imagem usando PVS. Essas VMs servem como dispositivos de destino PVS e o servidor PVS pode transmitir uma única imagem de disco compartilhada para elas.

    > **Observação:**
    >
    > Esta opção está disponível apenas para sites PVS registrados com o Citrix Cloud™ e está atualmente limitada a recursos do Azure.

- **Outro serviço ou tecnologia** Uma ferramenta que gerencia máquinas já existentes no data center. A Citrix recomenda que você use o Microsoft System Center Configuration Manager ou outro aplicativo de terceiros para garantir que as máquinas no catálogo sejam consistentes.

## Tipos de área de trabalho (experiência de área de trabalho)

Esta página aparece somente quando você está criando um catálogo contendo máquinas de SO de sessão única.

A página **Experiência da Área de Trabalho** determina o que ocorre cada vez que um usuário faz logon. Selecione uma das opções:

- Os usuários se conectam a uma nova área de trabalho (aleatória) cada vez que fazem logon.
- Os usuários se conectam à mesma área de trabalho (estática) cada vez que fazem logon.

## Imagem e perfil da máquina

Esta 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 mestre.** Uma imagem que ainda não passou pelo processo de preparação de imagem. O processo de preparação de imagem é iniciado automaticamente quando a criação do catálogo começa.

     > **Observação:**
     >
     > - Ao usar o MCS, não execute o Sysprep em imagens mestre.
     > - Se você especificar uma imagem mestre em vez de um instantâneo, o Web Studio cria um instantâneo, mas você não pode nomeá-lo.

   - **Imagem preparada.** Uma imagem que passou pelo processo de preparação de imagem e pode ser usada diretamente para a criação de VM. Optar por imagens preparadas em vez de imagens mestre durante a criação do catálogo garante uma criação de catálogo de máquinas mais rápida e confiável, juntamente com um gerenciamento simplificado do ciclo de vida da imagem.

> **Observação:**
>
> - VMs criadas usando imagens preparadas não suportam hibernação.
> - Atualmente, a criação de catálogos usando imagens preparadas está disponível apenas em ambientes Azure e VMware.

Para obter mais informações sobre como criar imagens preparadas, consulte Gerenciamento de imagens (visualização).

Ao selecionar uma imagem, você pode adicionar uma nota para a imagem selecionada, se necessário.

Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada. Não altere a seleção mínima padrão do VDA. No entanto, se você precisar usar uma versão anterior do VDA, consulte Versões do VDA e níveis funcionais.

Uma mensagem de erro aparece se você selecionar um instantâneo ou VM que não seja compatível com a tecnologia de gerenciamento de máquina selecionada anteriormente no assistente.

2. Para usar uma VM existente como perfil de máquina, selecione **Usar um perfil de máquina** e, em seguida, selecione a VM.

> **Observação:**
>
> Atualmente, o uso de perfis de máquina é restrito a VMs do Azure, AWS, GCP e VMware.

> Para implantações VMware, ao criar um catálogo de máquinas usando um perfil de máquina, você deve especificar a pasta onde deseja manter as máquinas virtuais.

Para fornecer o local da pasta da máquina virtual, no assistente de criação de catálogo, vá para a página **Máquinas Virtuais** e vá para a seção **Selecionar uma pasta para colocar as máquinas** e selecione o local da pasta da máquina virtual. Se não for especificado, o sistema considera a pasta do perfil de máquina selecionado como o local padrão.

3. Selecione o nível funcional mínimo para o catálogo. Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada.

## Máquinas

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

O título desta página depende do que você selecionou na página **Gerenciamento de Máquinas**: **Máquinas**, **Máquinas Virtuais** ou **VMs e usuários**.

**Ao usar MCS:**

- Especifique quantas máquinas virtuais criar. Digite **0** (zero) se não quiser criar nenhuma. Mais tarde, você pode criar VMs para um catálogo vazio executando **Adicionar máquinas**.
- Escolha a quantidade de memória (em MB) que cada VM terá.
- Cada VM criada tem um disco rígido. Seu tamanho é definido na imagem mestre. Você não pode alterar o tamanho do disco rígido no catálogo.
- Se sua implantação contiver mais de uma zona, você poderá selecionar uma zona para o catálogo.
- Se você estiver criando VMs de desktop estáticas, selecione um modo de cópia de máquina virtual. Consulte Modo de cópia de máquina virtual.
- Se você estiver criando VMs de desktop aleatórias que não usam vDisks, poderá configurar um cache para ser usado para dados temporários em cada máquina. Consulte Configurar cache para dados temporários.

**Ao usar outras ferramentas:**

Adicione (ou importe uma lista de) nomes de contas de máquina do Active Directory. Você pode alterar o nome da conta do Active Directory para uma VM depois de adicioná-la/importá-la. Se você especificou máquinas estáticas na página **Experiência da Área de Trabalho**, pode, opcionalmente, especificar o nome de usuário do Active Directory para cada VM que adicionar.

Depois de adicionar ou importar nomes, você pode usar o botão **Remover** para excluir nomes da lista, enquanto ainda estiver nesta página.

**Ao usar outras ferramentas (mas não MCS):**

Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada) ajudam a identificar máquinas que podem não ser elegíveis para adicionar ao catálogo ou que não

conseguem se registrar em um Delivery Controller. Para obter detalhes, consulte Versões de VDA e níveis funcionais.

### Adicionar SIDs ao criar máquinas virtuais

Agora você pode adicionar o parâmetro `ADAccountSid` para identificar exclusivamente as máquinas ao criar novas máquinas virtuais.

Para fazer isso:

1. Crie um catálogo com o tipo de identidade compatível.
2. Adicione máquinas ao catálogo usando `NewProvVM`. Por exemplo:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta AD que não está no pool de identidades do catálogo
- Uma conta AD que não está no estado disponível

### Modo de cópia da máquina virtual

O modo de cópia que você especifica na página **Máquinas** determina se o MCS cria clones finos (cópia rápida) ou espessos (cópia completa) a partir da imagem mestre. (Padrão = clones finos)

- Use clones de cópia rápida para um uso de armazenamento mais eficiente e criação de máquina mais rápida.
- Use clones de cópia completa para melhor recuperação de dados e suporte à migração, com IOPS potencialmente reduzidos após a criação das máquinas.

### Versões do VDA e níveis funcionais

O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto requer um novo VDA. A definição de um nível funcional torna todos os recursos introduzidos nessa versão (e posteriores, se o nível funcional não for alterado) disponíveis para as máquinas no catálogo. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não podem se registrar.

Um menu próximo à parte inferior da página **Máquinas** (ou **Dispositivos**) permite selecionar o nível mínimo de VDA. Isso define o nível funcional mínimo do catálogo. Por padrão, o nível funcional mais atual é selecionado para implantações locais. Se você seguir a recomendação da

Citrix de sempre instalar e atualizar VDAs e componentes principais para a versão mais recente, não precisará alterar essa seleção. No entanto, se você precisar continuar usando versões mais antigas do VDA, selecione o valor correto.

Uma versão do Citrix Virtual Apps and Desktops pode não incluir uma nova versão do VDA, ou o novo VDA não afeta o nível funcional. Nesses casos, o nível funcional pode indicar uma versão do VDA anterior aos componentes instalados ou atualizados. O artigo Novidades de cada versão indica qualquer alteração no nível funcional padrão.

O nível funcional selecionado afeta a lista de máquinas acima dele. Na lista, uma dica de ferramenta ao lado de cada entrada indica se o VDA da máquina é compatível com o catálogo naquele 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. É provável que essas máquinas não consigam se registrar em um Controller mais tarde. Alternativamente, você pode:

- Remova as máquinas que contêm VDAs mais antigos da lista, atualize seus VDAs e adicione-as novamente ao catálogo.
- Escolha um nível funcional inferior que impeça o acesso aos recursos mais recentes do produto.

Uma mensagem também é exibida se uma máquina não foi adicionada ao catálogo porque é do tipo de máquina incorreto. Os exemplos incluem tentar adicionar um servidor a um catálogo de SO de sessão única ou adicionar uma máquina de SO de sessão única originalmente criada para alocação aleatória a um catálogo de máquinas estáticas.

> **Importante:**

> Na versão 1811, um nível funcional extra foi adicionado: **1811 (ou mais recente)**. Esse nível é destinado ao uso com futuros recursos do Citrix Virtual Apps and Desktops. A seleção **7.9 (ou mais recente)** permanece como padrão. Esse padrão é válido para todas as implantações agora.

> Se você selecionar **1811 (ou mais recente)**, quaisquer versões anteriores de VDA nesse catálogo não poderão se registrar em um Controller. No entanto, se o catálogo contiver apenas VDAs na versão 1811 ou versões posteriores compatíveis, todos eles serão elegíveis para registro. Isso inclui catálogos que contêm VDAs configurados para versões

posteriores do Citrix Virtual Apps and Desktops, incluindo a versão 1903 e outras versões 19XX antes da versão atual.

### Configurar cache para dados temporários

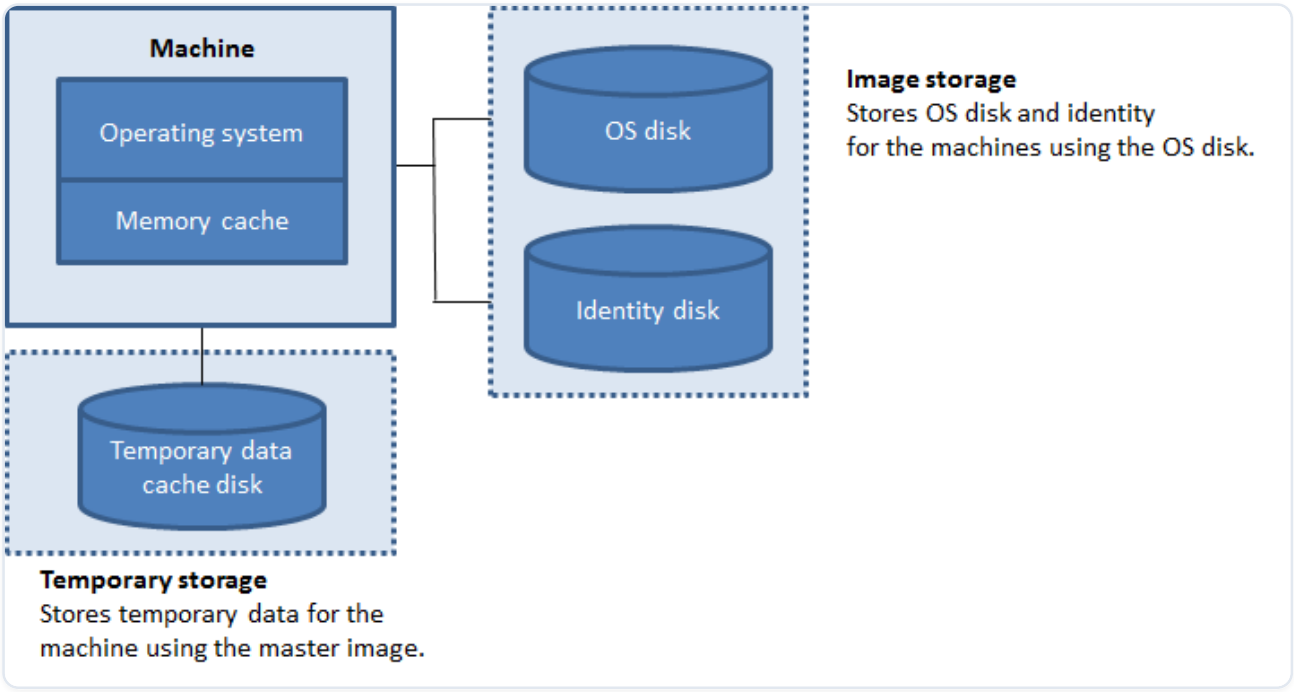
O cache de dados temporários localmente na VM é opcional. Você pode habilitar o uso do cache de dados temporários na máquina ao usar o MCS para gerenciar máquinas agrupadas (não dedicadas) em um catálogo. Se o catálogo usar uma conexão que especifica armazenamento para dados temporários, você poderá habilitar e configurar as informações do cache de dados temporários ao criar o catálogo.

**Importante:**

Esse recurso requer um driver MCS I/O atual. A instalação desse driver é uma opção ao instalar ou atualizar um VDA. Por padrão, esse driver não é 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 em disco (GB)**. Por padrão, as duas opções estão desmarcadas. Para habilitar a opção Memória alocada para cache (MB), selecione a caixa de seleção Tamanho do cache em disco (GB). Se a caixa de seleção **Tamanho do cache em disco** não estiver selecionada, a opção **Memória alocada para cache** ficará esmaecida. Dependendo do tipo de conexão, os valores padrão para essas 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 quaisquer aplicativos 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 selecionar a caixa de seleção Tamanho do cache em disco e a caixa de seleção Memória alocada para o cache, os dados temporários não serão armazenados em cache. Eles são gravados diretamente no disco de diferença (localizado no armazenamento do SO) para cada VM. (Esta é a ação de provisionamento na versão 7.8 e anteriores.)
- Se você selecionar a caixa de seleção Tamanho do cache em disco e a caixa de seleção Memória alocada para cache, os dados temporários serão gravados inicialmente no cache de memória. Quando o cache de memória atinge seu limite configurado (o valor de Memória alocada para cache), os dados mais antigos são movidos para o disco de cache de dados temporários.

**Importante:**

- Se o cache de disco ficar sem espaço, a sessão do usuário se torna inutilizável.
- Este recurso não está disponível ao usar uma conexão de host Nutanix.
- Você não pode alterar os valores de cache em um catálogo de máquinas depois que a máquina é criada.

**Observação:**

- A configuração do cache de write-back com apenas um cache em disco e sem cache de memória foi descontinuada. Para habilitar um cache para dados temporários, recomendamos selecionar **Tamanho do cache em disco (GB)** e **Memória alocada para 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 habilitar a opção Memória alocada para cache, considere aumentar a quantidade total de memória em cada máquina.
- Alterar o tamanho do cache de disco de seu valor padrão pode afetar o desempenho. O tamanho deve corresponder aos requisitos do usuário e à carga colocada na máquina.

## NIC

Esta página não aparece ao criar catálogos de Acesso Remoto a PC.

Na página **Placas de Interface de Rede**, se você planeja usar várias NICs, associe uma rede virtual a cada placa. Por exemplo, você pode atribuir uma placa para acessar uma rede segura específica e outra placa para acessar uma rede mais comumente usada. Você também pode adicionar ou remover NICs desta página.

## Contas de máquina

Esta página aparece apenas ao criar catálogos de Acesso Remoto a PC.

Na página **Contas de Máquina**, especifique as contas de máquina do Active Directory ou Unidades Organizacionais (OUs) a serem adicionadas que correspondem a usuários ou grupos de usuários. Não use uma barra (/) em um nome de OU.

Ao adicionar OUs, você pode fazer o seguinte se o domínio não for exibido na lista:

- Pesquise-o 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 deseja usar o gerenciamento de energia, mas uma conexão adequada ainda não foi configurada, você pode criar essa conexão mais tarde e, em seguida, editar o catálogo de máquinas para atualizar as configurações de gerenciamento de energia.

# Identidades de máquina

Esta página aparece apenas 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 configurar as configurações nesta página é o seguinte:

1. Selecione uma identidade na lista.
2. Indique se deseja criar contas ou usar as existentes, e o local (domínio) para essas contas.

Você pode selecionar uma das seguintes opções:

- **Active Directory local**. Máquinas de propriedade de uma organização e conectadas com uma conta do Active Directory que pertence a essa organização. Elas existem localmente.
- **Unido ao Azure Active Directory Híbrido**. Máquinas de propriedade de uma organização e conectadas com uma conta do Active Directory Domain Services que pertence a essa organização. Elas existem na nuvem e localmente. Para obter informações sobre os requisitos, limitações e considerações, consulte Unido ao Azure Active Directory Híbrido.

  > **Observação:**
  >
  > - Antes de usar o ingresso híbrido no Azure Active Directory, certifique-se de que seu ambiente Azure atenda aos pré-requisitos. Consulte `<https://docs.microsoft.com/pt-br/azure/active-directory/devices/hybrid-azuread-join-managed-domains>`.
  > - Esta opção exige que a imagem mestre atenda ao pré-requisito do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft: `<https://learn.microsoft.com/pt-br/azure/active-directory/devices/concept-azure-ad-join-hybrid>`.

> **Importante:**

- Se você selecionar **Active Directory local** ou **Ingresso híbrido no Azure Active Directory** como tipo de identidade, cada máquina no catálogo deve ter uma conta de computador do Active Directory correspondente.

Se você criar contas, deverá ter permissão para criar contas de computador na UO onde as máquinas residem. Cada máquina no catálogo deve ter um nome exclusivo. Especifique o esquema de nomenclatura de conta para as máquinas que você deseja criar. Para obter mais informações, consulte Esquema de nomenclatura de conta de máquina.

**Observação:**

Certifique-se de que os nomes das UOs não usem barras ( `/` ).

Se você usar contas existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo .csv contendo nomes de contas. O conteúdo do arquivo importado deve usar o formato:

- ADcomputeraccountname.domain

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 que contêm máquinas físicas ou existentes, selecione ou importe contas existentes e atribua cada máquina a uma conta de computador do Active Directory e a uma conta de usuário.

### Esquema de nomenclatura de contas de máquina

Cada máquina em um catálogo deve ter um nome exclusivo. Você deve especificar um esquema de nomenclatura de contas de máquina ao criar um catálogo. Use curingas (sinais de cerquilha) como espaços reservados para números ou letras sequenciais que aparecem no nome.

Ao especificar um esquema de nomenclatura, esteja ciente das seguintes regras:

- O esquema de nomenclatura deve conter pelo menos um curinga. Você deve colocar todos os curingas juntos.

- O nome completo, incluindo curingas, deve conter no mínimo 2 e no máximo 15 caracteres. Deve incluir pelo menos um caractere não numérico e um caractere # (curinga).
- O nome não deve incluir espaços ou qualquer um dos seguintes caracteres: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`.
- O nome não pode terminar com um hífen (-).

Além disso, deixe espaço suficiente para crescimento ao especificar o esquema de nomenclatura. Considere este exemplo: Se você criar 1.000 contas de máquina com o esquema "veryverylong#", o último nome de conta criado (veryverylong1000) contém 16 caracteres. Portanto, o esquema de nomenclatura resulta em um ou mais nomes de máquina que excedem o máximo de 15 caracteres.

Você pode indicar se os valores sequenciais são números (0-9) ou letras (A-Z):

- **0-9**. Se selecionado, os curingas especificados se resolvem em números sequenciais.

  > **Nota:**
  >
  > Se houver apenas um curinga (#), os nomes das contas começam com 1. Se houver dois, os nomes das contas começam com 01. Se houver três, os nomes das contas começam com 001, e assim por diante.

- **A-Z**. Se selecionado, os curingas especificados se resolvem em letras sequenciais.

Por exemplo, um esquema de nomenclatura de PC-Sales-## (com **0-9** selecionado) resulta em contas nomeadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

Opcionalmente, você pode especificar com o que os nomes das contas começam.

- Se você selecionar **0-9**, as contas são nomeadas sequencialmente, começando com os números especificados. Insira um ou mais dígitos, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira dois dígitos ou mais.
- Se você selecionar **A-Z**, as contas são nomeadas sequencialmente, começando com as letras especificadas. Insira uma ou mais letras, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira duas letras ou mais.

## Credenciais de domínio

Selecione **Inserir credenciais** e insira as credenciais de um administrador com permissão para realizar operações de conta no domínio do Active Directory de destino.

Use a opção **Verificar nome** para verificar se o nome de usuário é válido ou exclusivo. A opção é útil, por exemplo, quando:

- O mesmo nome de usuário existe em vários domínios. Você é solicitado a selecionar o usuário desejado.
- Você não consegue se lembrar do nome de domínio. Você pode inserir o nome de usuário sem especificar o nome de domínio. Se a verificação for aprovada, o nome de domínio será preenchido automaticamente.

> **Nota:**

> Se o tipo de identidade selecionado em **Identidades da Máquina** for **Ingresso híbrido no Azure Active Directory**, as credenciais inseridas devem ter recebido a permissão `Write userCertificate`.

## Resumo, nome e descrição

Na página **Resumo**, revise as configurações especificadas. 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 **Catálogos de Máquinas**, o novo catálogo aparece com uma barra de progresso em linha.

Para visualizar os detalhes do progresso da criação:

1. Passe o mouse sobre o catálogo de máquinas.
2. Na dica de ferramenta que aparece, clique em **Exibir detalhes**.

   Um gráfico de progresso passo a passo aparece onde você pode ver o seguinte:

   - Histórico de etapas
   - Progresso e tempo de execução da etapa atual
   - Etapas restantes

## Sincronização de tempo do MCS

A sincronização de tempo é determinada pela imagem mestre e pelo tipo de catálogo unido à identidade da máquina. Você obtém o seguinte método de sincronização de tempo de acordo com a imagem mestre e o catálogo:

| IMAGEM MESTRE | CATÁLOGO | MÉTODO DE SINCRONIZAÇÃO DE TEMPO RESULTANTE |
|---|---|---|
| NDJ | AD ou Azure AD Híbrido | Por padrão, NT5DS. Você pode desabilitar o MCS de alterar a configuração de sincronização de tempo usando as configurações de registro na imagem mestre |
| NDJ | NDJ ou Azure AD | O mesmo que a configuração original de sincronização de tempo |
| AD ou Azure AD Híbrido | AD ou Azure AD Híbrido | O mesmo que a configuração original de sincronização de tempo |
| Azure AD | Azure AD | O mesmo que a configuração original de sincronização de tempo |

**Nota:**

A sincronização de tempo original é controlada pela seguinte configuração de registro e não pode ser alterada:

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

Valor: MaxAllowedPhaseOffset, MaxNegPhaseCorrection e MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

Valor: Type

Para desabilitar o MCS de alterar a configuração de sincronização de tempo, defina o valor da seguinte configuração de registro na imagem mestre:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nome: TimeSyncMethodKeep
- Tipo: DWORD
- 0 (Ou, valor TimeSyncMethodKeep não configurado): Não mantém a configuração original de sincronização de tempo.
- 1: Mantém a configuração original de sincronização de tempo e os valores padrão dos parâmetros.

## Consideração importante sobre a definição de propriedades personalizadas

As propriedades personalizadas devem ser definidas corretamente em `New-ProvScheme` e `Set-ProvScheme` em ambientes GCP e Azure. Se você especificar uma propriedade ou propriedades personalizadas inexistentes, receberá a seguinte mensagem de erro e os comandos falharão ao serem executados.

- No Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- No GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

## Solução de problemas

**Importante:**

Após criar o catálogo de máquinas usando o Web Studio, você não pode mais usar o comando PowerShell `Get-ProvTask` para recuperar as tarefas associadas à criação do catálogo de máquinas. Essa restrição é resultado do Web Studio excluir essas tarefas após

> a criação do catálogo de máquinas, independentemente de o catálogo ter sido criado com sucesso.

> A Citrix recomenda coletar logs para ajudar a equipe de Suporte a fornecer soluções. Ao usar o Citrix Provisioning, use o seguinte procedimento para gerar arquivos de log:

1. Na imagem mestre, crie a seguinte chave de registro com o valor 1 (como um valor DWORD (32 bits)): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Desligue a imagem mestre e crie um instantâneo.
3. No Delivery Controller, execute o seguinte comando PowerShell: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Crie um catálogo com base nesse instantâneo.
5. Quando a VM de preparação for criada no hipervisor, faça login e extraia os seguintes arquivos da raiz de `C:\`: Image-prep.log e PvsVmAgentLog.txt.
6. Desligue a máquina, momento em que ela relata a falha.
7. Execute o seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

### Problemas de preparação de imagem

Como o MCS cria muitas máquinas a partir de uma única imagem, algumas etapas são executadas para garantir que todas as máquinas sejam únicas 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 ao 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, garantindo que a VM preparada seja anexada apenas ao disco recém-copiado.

Um pequeno disco de *instrução*, contendo as etapas necessárias para executar a preparação da imagem, é anexado à VM preparada. Esta VM preparada inicia e o processo de preparação da imagem começa. A preparação da imagem inclui os seguintes processos:

- Habilitar DHCP. A habilitação do DHCP garante que as máquinas provisionadas não causem conflitos de endereço IP. O DHCP é habilitado em todas as placas de rede.
- Rearmamento do KMS do Microsoft Windows. O rearmamento do KMS garante que o Microsoft Windows esteja licenciado corretamente. O SO rearmado é invocado para que seja relatado corretamente como uma nova instância ao servidor de licenças KMS.
- Rearmamento do KMS do Microsoft Office (se o Microsoft Office estiver instalado). O rearmamento do Microsoft Office garante que qualquer versão do Microsoft Office (2010+) seja registrada corretamente com seu servidor KMS. Uma vez invocado o rearmamento do Microsoft Office, ele é relatado como uma nova instância ao servidor de licenças KMS.

> **Dica:**

> Quando o processo de preparação da imagem termina, o disco de instrução é obtido do hipervisor. O hipervisor contém as informações coletadas do processo de preparação da imagem.

> Existem várias razões pelas quais a fase de preparação da imagem pode falhar. Uma mensagem de falha semelhante à seguinte aparece: Image Preparation Office Rearm Failed.

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 de placas de rede Dell SonicWall. A operação falhou porque uma placa SonicWall é uma placa de rede de firewall, então configurar a placa para DHCP não faz sentido, pois ela só suporta DHCP. Isso foi corrigido em versões posteriores do Citrix Virtual Apps and Desktops. No entanto, se for observado em outros tipos de placas de rede, deve ser relatado à Citrix através dos fóruns ou do seu contato de suporte.

> **Observação:**

> Esta configuração do PowerShell nos exemplos a seguir é aplicada ao site do Citrix Virtual Apps and Desktops, portanto, afeta todos os novos catálogos e atualizações de imagem realizadas em catálogos existentes.

> Se você encontrar esse problema com outras placas de rede, poderá resolvê-lo executando um comando PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP
```

### Rearm do Microsoft Office

Existem várias falhas de rearm do KMS que podem ocorrer durante a fase de rearm do Microsoft Office. As principais falhas são:

- Alguns runtimes do Microsoft Office, por exemplo, **Access Runtime**, podem invocar o rearm do Office, fazendo com que ele falhe.
- Uma versão KMS do Microsoft Office não está instalada.
- Contagem de rearm excedida.

Se o erro for um falso positivo, você pode resolvê-lo executando o seguinte comando PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm
```

### Rearm do Microsoft Windows

Várias falhas de KMS podem ocorrer durante a fase de rearm do Microsoft Windows. As principais falhas são:

- A versão do Windows instalada não está ativada usando KMS. Por exemplo, ela usa uma Chave de Ativação Múltipla (MAK).
- Contagem de rearmamento excedida.

Se a versão do Microsoft Windows estiver corretamente licenciada, você pode limpar o rearmamento do SO executando o seguinte comando PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm
```

### Instâncias de falha completa

A máquina de preparação de imagem não está conectada à rede por design, o que significa que, às vezes, a etapa de preparação de imagem pode apenas relatar uma falha completa. Um exemplo desse tipo de falha é: A preparação da Imagem da VM Mestra falhou. Certifique-se de

que a imagem selecionada tenha um SO compatível (por exemplo, Windows 7) e a versão correta do VDA (7.0 ou posterior) instalada.

As principais razões para uma falha completa são:

#### O VIRTUAL DELIVERY AGENT (VDA) NÃO ESTÁ INSTALADO, OU A VERSÃO 5.X DO VDA ESTÁ INSTALADA

Se o VDA 7.x não estiver instalado na imagem mestra, a preparação da imagem expira após 20 minutos e relata o erro acima. Isso ocorre porque não há software instalado na imagem mestra para executar a etapa de preparação da imagem e relatar sucesso ou falha. Para resolver isso, certifique-se de que o VDA (versão mínima 7) esteja instalado no snapshot selecionado como imagem mestra.

#### POLÍTICA `DISKPART SAN`

Toda a etapa de preparação da imagem pode falhar devido à política `DISKPART SAN` definida na imagem mestra. Se não estiver configurada para colocar o disco de instruções de preparação da imagem online, a máquina é desligada e a preparação da imagem relata uma falha após 20 minutos. Para verificar isso na imagem mestra, execute os seguintes comandos:

```
C:\>; Diskpart.exe

DISKPART>; San
```

Este comando retorna a política atual. Se não for *Online All*, altere-o executando o seguinte comando:

```
DISKPART>; San policy=OnlineAll
```

Desligue a imagem mestra, crie um snapshot dessa máquina e use-o como a imagem base 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 pode ignorar o processo de preparação da imagem ao criar um catálogo MCS. No entanto, ignorar esse processo pode causar problemas com o licenciamento KMS e a rede (DHCP) em seu site. Use o seguinte comando PowerShell:

```
Set-ProvServiceConfigurationData -Name
ImageManagementPrep_DoImagePreparation -Value $false
```

Sempre que possível, colete logs para a equipe de Suporte da Citrix. Relate o problema à Citrix por meio dos fóruns ou por meio de seu contato de suporte. Para coletar logs:

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:\:

```
Image-prep.log

PvsVmAgentLog.txt
```

Desligue a máquina. Neste ponto, ela relata a falha.

Execute o seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem:

`Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`

## Próximos passos

Para obter informações sobre como criar catálogos de serviços de nuvem específicos, consulte:

- Criar um catálogo AWS
- Criar um catálogo XenServer
- Criar um catálogo Google Cloud Platform
- Criar um catálogo Microsoft Azure
- Criar um catálogo Microsoft System Center Virtual Machine Manager
- Criar um catálogo Nutanix
- Criar um catálogo VMware

Se este for o primeiro catálogo criado, o Web Studio o guiará para (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html).

Para revisar todo o processo de configuração, consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html).

Você pode criar um catálogo do Citrix Provisioning usando o Web Studio e o PowerShell. Esta implementação oferece as seguintes vantagens:

- Um único console unificado para gerenciar catálogos MCS e Citrix Provisioning.
- Ter novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Atualmente, este recurso está disponível apenas para cargas de trabalho do Azure e VMware. No entanto, em ambientes VMware, você pode atualmente criar os catálogos usando apenas comandos PowerShell. Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

## Mais informações

- Criar e gerenciar conexões e recursos
- Gerenciar catálogos de máquinas

## Criar um catálogo AWS

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização AWS.

> **Observação:**
>
> Antes de criar um catálogo AWS, você precisa concluir a criação de uma conexão com a AWS. Consulte Conexão com a AWS.

### Limitação

A partir do Citrix Virtual Apps and Desktops™ 2203 LTSR e posterior, o plug-in MCS AWS faz a chamada de API AWS `DescribeInstanceTypes` e, se for bem-sucedida, o MCS usa o nome do inventário criado a partir da resposta da API.

Portanto, ao fazer upgrade do CVAD 1912 para 2203 ou posterior, desabilite a permissão `DefineInstanceType` na AWS e, em seguida, atualize o catálogo existente usando o comando `Set-ProvScheme` para corresponder ao esquema de nomenclatura da AWS. Em seguida,

adicione as permissões `DescribeInstanceType` de volta após a conclusão da atualização do catálogo e o serviço oferecido corresponder ao esquema de nomenclatura da AWS.

### Configuração de rede durante a preparação da imagem

Durante a preparação da imagem, uma máquina virtual (VM) de preparação é criada com base na VM original. Esta VM de preparação é desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. Este grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, onde GUID é gerado aleatoriamente.

### Configurar a tenancy da AWS

A AWS oferece as seguintes opções de tenancy:

- Tenancy compartilhada (o tipo padrão): Várias instâncias do Amazon EC2 de diferentes clientes podem residir na mesma peça de hardware físico.
- Tenancy dedicada: Suas instâncias EC2 são executadas apenas em hardware com outras instâncias que você implantou. Outros clientes não usam a mesma peça de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando o PowerShell.

#### Configurar a tenancy de host dedicado da AWS usando o PowerShell

Você pode criar um catálogo de máquinas com tenancy de host definida via PowerShell.

Um host dedicado Amazon é um servidor físico com capacidade de instância que é totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM.

Hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado de tipos de instância C4 Large é limitado a executar 16 instâncias. Consulte o site da AWS para obter mais informações.

Os requisitos para provisionamento em hosts AWS incluem:

- Uma imagem BYOL (traga sua própria licença) (AMI) importada. Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para satisfazer as solicitações de provisionamento.
- habilitar o **posicionamento automático**.

Para provisionar para um host dedicado no AWS usando PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro `TenancyType` definido como *Host*.

Consulte a Documentação do Desenvolvedor Citrix para obter mais informações.

### Capturar propriedades da máquina de AMIs

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) no AWS, você seleciona uma AMI para representar a imagem mestre/golden desse catálogo. Dessa AMI, o MCS usa um snapshot do disco. Em versões anteriores, se você quisesse funções ou tags em suas máquinas, você usaria o console do AWS para configurá-las individualmente. Essa funcionalidade é habilitada por padrão.

> **Dica:**
>
> Para usar a captura de propriedades de instância do AWS, você deve ter uma VM associada à AMI.

> Para melhorar esse processo, o **MCS lê** as propriedades da instância da qual a AMI foi tirada e aplica a função e as tags do Identity Access Management (IAM) da máquina às máquinas provisionadas para um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo encontra a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são então armazenadas em um Modelo de Inicialização do AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades de instância capturadas.

As propriedades capturadas incluem:

- Funções IAM – aplicadas a instâncias provisionadas.
- Tags - aplicadas a instâncias provisionadas, seus discos e NICs. Essas tags são aplicadas a recursos transitórios do Citrix®, incluindo: buckets e objetos S3, e AMIs, snapshots e modelos de inicialização.

> **Dica:**
>
> A marcação de recursos transitórios do Citrix é opcional e é configurável usando a propriedade personalizada `AwsOperationalResourcesTagging`.

### Capturar a propriedade da instância do AWS

Você pode usar esse recurso especificando uma propriedade personalizada, `AwsCaptureInstanceProperties`, ao criar um esquema de provisionamento para uma conexão de hospedagem AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" …<standard provscheme parameters
```

Consulte a Documentação do Desenvolvedor Citrix para obter mais informações.

> **Observação:**
>
> O `AwsCaptureInstanceProperties` está obsoleto. Recomendamos usar perfis de máquina para especificar propriedades de máquina para VMs.

### Capturar propriedades de máquina de perfis de máquina

Ao criar um catálogo para provisionar máquinas AWS usando MCS, você pode usar um perfil de máquina para predefinir certas configurações de propriedade da máquina.

Para fazer isso, siga estas etapas:

1. Armazene os perfis de máquina na mesma zona de disponibilidade que os recursos onde você está criando este catálogo.
2. Na página **Modelo de Máquina** do assistente de criação de catálogo, selecione **Usar um perfil de máquina**. Os perfis de máquina localizados na mesma zona disponível que os recursos selecionados são exibidos.
3. Selecione um perfil de máquina conforme necessário.

> **Observação:**
>
> Você pode usar um perfil de máquina ou uma AMI para capturar propriedades da máquina. No Web Studio, ao selecionar **Usar um perfil de máquina**, a opção **Aplicar propriedades do modelo de máquina a máquinas virtuais** é automaticamente ocultada.

### Marcar recurso operacional AWS

Ao criar um catálogo para provisionar máquinas na AWS usando MCS, você pode controlar se deve aplicar a função IAM e as propriedades de tag a essas máquinas. Você também pode controlar se deve aplicar tags de máquina a recursos operacionais.

Uma Amazon Machine Image (AMI) representa um tipo de appliance virtual usado para criar uma máquina virtual dentro do ambiente Amazon Cloud, comumente referido como EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Ao criar um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem dourada para esse catálogo.

> **Importante:**
>
> A criação de catálogos capturando uma propriedade de instância e um modelo de inicialização é necessária para usar a marcação de recursos operacionais.

> Para criar um catálogo AWS, você deve primeiro criar uma AMI para a instância que deseja que seja a imagem dourada. O MCS lê as tags dessa instância e as incorpora no modelo de inicialização. As tags do modelo de inicialização são então aplicadas a todos os recursos Citrix criados em seu ambiente AWS, incluindo:

- Máquinas Virtuais
- Discos de VM
- Interfaces de rede de VM
- Buckets S3
- Objetos S3
- Modelos de inicialização
- AMIs

#### Marcar um recurso operacional

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell a partir do host DDC.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.

Para marcar um recurso para uma VM provisionada, use a nova propriedade personalizada `AwsOperationalResourcesTagging`. A sintaxe para esta propriedade é:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo AWS

### Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das fontes de perfil da máquina (instância de VM AWS ou versão de modelo de inicialização AWS). Este recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes.

**Observação:**

- No console do AWS EC2, você não pode ver os valores de **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver as especificações da tag.
- Se uma fonte de perfil de máquina (VM ou versão de modelo de inicialização) tiver duas interfaces de rede (eni-1 e eni-2), e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, então a VM receberá as tags de ambas as interfaces de rede.

### Criar um catálogo usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services™ (MCS) na AWS, agora você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume EBS, tipo de instância, otimização EBS e outras configurações AWS suportadas. Ao editar o

catálogo, o perfil de máquina das máquinas provisionadas pode ser alterado fornecendo uma VM ou modelo de inicialização diferente.

> **Observação:**
>
> As propriedades do volume EBS são derivadas apenas de um perfil de máquina.

### Considerações importantes

As considerações importantes ao criar um catálogo de máquinas MCS:

- Se você adicionar parâmetros de propriedade de hardware da máquina nos comandos `New-ProvScheme` e `Set-ProvScheme`, os valores fornecidos nos parâmetros sobrescreverão os valores no perfil da máquina.
- Se você definir `AwsCaptureInstanceProperties` como `true` e não definir a propriedade `MachineProfile`, então apenas as funções e tags do IAM serão capturadas.
- Você não pode definir `AwsCaptureInstanceProperties` e `MachineProfile` ao mesmo tempo.

  > **Nota:
  >
  > O `AwsCaptureInstanceProperties` está obsoleto.

- Você deve fornecer explicitamente os valores das seguintes propriedades:
  - TenancyType
  - Grupo de Segurança
  - NIC ou Rede Virtual
- Você pode habilitar `AwsOperationalResourcesTagging` somente se habilitar `AwsCaptureInstanceProperties` ou especificar um perfil de máquina.

As considerações importantes após criar um catálogo de máquinas MCS:

- Somente as novas VMs adicionadas ao catálogo são afetadas pela alteração.
- Você não pode alterar um catálogo de baseado em perfil de máquina para um catálogo não baseado em perfil de máquina.

### Criar um catálogo de máquinas usando um perfil de máquina

Para criar um catálogo de máquinas usando um perfil de máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. Execute o comando New-ProvScheme. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. Conclua a criação do catálogo. Para obter mais informações, consulte Citrix PowerShell SDK.

Para atualizar o perfil de máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
```

```
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

### Criar um catálogo com versão de modelo de inicialização

Você pode criar um catálogo de máquinas MCS com uma versão de modelo de inicialização como entrada de perfil de máquina. Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM.

No console AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de inicialização junto com o número da versão. Ao especificar a versão do modelo de inicialização como entrada de perfil de máquina durante a criação ou atualização de um catálogo de máquinas, as propriedades dessa versão do modelo de inicialização são copiadas para as VMs VDA provisionadas.

As seguintes propriedades podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidas nos comandos `New-ProvScheme` ou `Set-ProvScheme`, elas terão precedência sobre os valores do perfil da máquina dessas propriedades.

- Oferta de Serviço
- Redes
- Grupos de Segurança
- Tipo de Tenancy

> **Nota:**

> Se a oferta de serviço não for fornecida no modelo de inicialização do perfil da máquina ou como um parâmetro no comando `New-ProvScheme`, você receberá um erro apropriado.

> Para criar um catálogo usando a versão do modelo de inicialização como entrada de perfil de máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Obtenha a lista de versões de modelo de inicialização de um modelo de inicialização. Por exemplo:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão de modelo de inicialização como entrada de perfil de máquina. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

Você também pode substituir parâmetros como oferta de serviço, grupos de segurança, tenancy e redes. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion" `

-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large
Instance.serviceoffering"
```

6. Registre o esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Conclua a criação do catálogo. Para mais informações, consulte Citrix PowerShell SDK

Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- Para atualizar a entrada de um catálogo de perfil de máquina de uma versão de modelo de inicialização para uma VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

### Filtrar instâncias de VM

Uma instância AWS EC2 que você usa como VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criado e funcione corretamente. Para listar as instâncias AWS EC2 que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode paginar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

**Paginação:**

**Get-HypInventoryItem** oferece suporte a dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens ignorar desde o início absoluto (ou fim absoluto) da lista no hipervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:

- `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.
- `-ContinuationToken`: Retorna os itens imediatamente depois (ou antes, se `ForwardDirection` for **false**), mas não incluindo o item fornecido em `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem o `TotalItemsCount` e o `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- Para retornar um array de registros terminando com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- Para retornar um array de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

**Filtragem:**

Os seguintes parâmetros opcionais adicionais são suportados para filtragem. Você pode combinar esses parâmetros com as opções de paginação.

- `-ContainsName "my_name"`: Se a string fornecida corresponder a parte de um nome de AMI, a AMI será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **Nota:**
>
> Dois valores de tag são suportados. O valor da tag **Não Marcado** corresponde a itens que não possuem a tag fornecida em sua lista de tags. O valor da tag **Todos os valores** corresponde a itens que possuem a tag, independentemente do valor da tag. Caso contrário, a correspondência ocorre apenas se o item tiver a tag e o valor for igual ao que é fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

**Filtragem no parâmetro AdditionalData:**

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em AdditionalData. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs são incluídas com um campo `AdditionalData` chamado **Aviso**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com a AWS
- Criar catálogos de máquinas

## Criar um catálogo XenServer®

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização XenServer.

> **Observação:**
>
> Antes de criar um catálogo XenServer, você precisa concluir a criação de uma conexão com o XenServer. Consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-citrix-hypervisor.html).

### Criar um catálogo de máquinas usando uma conexão XenServer

Máquinas com capacidade de GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure máquinas com capacidade de GPU para permitir que a VM opere com software que usa a GPU para operações.

1. No XenCenter®, crie uma VM com VGA padrão, redes e vCPU.
2. Atualize a configuração da VM para habilitar o uso de GPU (seja Passthrough ou vGPU).
3. Instale um sistema operacional compatível e habilite o RDP.
4. Instale o Citrix VM Tools e os drivers NVIDIA.
5. Limpe o Console de Administração do Virtual Network Computing (VNC) para otimizar o desempenho e, em seguida, reinicie a VM.

6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e, em seguida, reinicie a VM.
7. Opcionalmente, crie um snapshot para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente que são configurados no XenCenter e usam recursos de GPU.

### Limitações

- Se uma implantação do Citrix Virtual Apps and Desktops com suas VMs hospedadas no Citrix Hypervisor 8.2 usar vários SRs GFS2 em um único catálogo MCS, as VMs no catálogo não poderão acessar os VDIs durante a implantação. O erro “VDI está atualmente em uso” é relatado.
- O XenServer não oferece suporte a VMs de clone completo do MCS com SRs GFS2.

Para obter mais informações, consulte Restrições.

### Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o MCS, você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Se o parâmetro `MachineProfile` não for usado, as propriedades de hardware serão capturadas da VM ou instantâneo da imagem mestre.

> **Observação:**
>
> Atualmente, você pode usar apenas uma VM como entrada de perfil de máquina.

> Você pode configurar explicitamente os seguintes parâmetros para sobrescrever os valores dos parâmetros na entrada do perfil da máquina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Para criar um catálogo com um perfil de máquina:

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*`.

3. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas. Por exemplo:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Crie as contas de computador AD necessárias no Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. Registre o esquema de provisionamento como um catálogo de broker. Por exemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. Adicione VMs ao catálogo.

Para atualizar um catálogo com um novo perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Para obter mais informações sobre o comando Set-ProvScheme, consulte Set-ProvScheme.

**Observação:**

- O comando `Set-ProvScheme` neste caso não altera o perfil da máquina das VMs existentes no catálogo. Apenas as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.
- Você não pode converter um catálogo de máquinas baseado em perfil de máquina para um catálogo de máquinas não baseado em perfil de máquina.

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo XenServer

### Mais informações

- Criar e gerenciar conexões e recursos

- Conexão com XenServer
- Criar catálogos de máquinas

## Criar um catálogo do Google Cloud Platform

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

> **Nota:**
>
> Antes de criar um catálogo do Google Cloud Platform (GCP), você precisa concluir a criação de uma conexão com o GCP. Consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-gcp.html).

### Prepare uma instância de VM mestre e um disco persistente

> **Dica:**
>
> Disco persistente é o termo do Google Cloud para disco virtual.

> Para preparar sua instância de VM mestre, crie e configure uma instância de VM com propriedades que correspondam à configuração desejada para as instâncias VDA clonadas em seu catálogo de máquinas planejado. A configuração não se aplica apenas ao tamanho e tipo da instância. Ela também inclui atributos da instância, como metadados, tags, atribuições de GPU, tags de rede e propriedades da conta de serviço.

Como parte do processo de masterização, o MCS usa sua instância de VM mestre para criar o *modelo de instância* do Google Cloud. O modelo de instância é então usado para criar as instâncias VDA clonadas que compõem o catálogo de máquinas. As instâncias clonadas herdam as propriedades (exceto as propriedades de VPC, sub-rede e disco persistente) da instância de VM mestre a partir da qual o modelo de instância foi criado.

Depois de configurar as propriedades da instância de VM mestre de acordo com suas especificações, inicie a instância e, em seguida, prepare o disco persistente para a instância.

Recomendamos que você crie manualmente um instantâneo do disco. Isso permite que você use uma convenção de nomenclatura significativa para rastrear versões, oferece mais opções para gerenciar versões anteriores da sua imagem mestre e economiza tempo na criação do catálogo de máquinas. Se você não criar seu próprio instantâneo, o MCS criará um instantâneo temporário para você (que é excluído no final do processo de provisionamento).

### Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas usando o Web Studio
- Criar um catálogo de máquinas usando o PowerShell

#### Criar um catálogo de máquinas usando o Web Studio

> **Observação:**

> Crie seus recursos antes de criar um catálogo de máquinas. Use as convenções de nomenclatura estabelecidas pelo Google Cloud ao configurar catálogos de máquinas. Consulte Diretrizes de nomenclatura de buckets e objetos para obter mais informações.

> Siga as orientações em Criar catálogos de máquinas. A descrição a seguir é exclusiva para catálogos do Google Cloud.

1. Faça login no Web Studio e selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione **Criar Catálogo de Máquinas** na barra de ações.
3. Na página **Sistema Operacional**, selecione **SO de várias sessões** e, em seguida, selecione **Avançar**.
    - O Citrix Virtual Apps and Desktops™ também oferece suporte a SO de sessão única.
4. Na página **Gerenciamento de Máquinas**, selecione as opções **Máquinas que têm o gerenciamento de energia ativado** e **Citrix Machine Creation Services™** e, em seguida, selecione **Avançar**. Se houver vários recursos, selecione um no menu.
5. Na página **Imagem**, conclua estas etapas conforme necessário e, em seguida, clique em **Avançar**.

a. Selecione um instantâneo ou VM como a imagem mestre. Se você quiser usar a funcionalidade de locação única, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente. Consulte Habilitar seleção de zona.

b. Para usar uma VM existente como perfil de máquina, selecione Usar um perfil de máquina e, em seguida, selecione a VM.

> **Observação:**
>
> Atualmente, as VMs neste catálogo herdam as configurações de ID do conjunto de criptografia de disco, tamanho da máquina, tipo de armazenamento e zona do perfil da máquina.

c. Selecione o nível funcional mínimo para o catálogo. Para usar a funcionalidade de locação única, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente.

6. Na página **Tipos de Armazenamento**, selecione o tipo de armazenamento usado para conter o sistema operacional para este catálogo de máquinas. Cada uma das seguintes opções de armazenamento tem características únicas de preço e desempenho. (Um disco de identidade é sempre criado usando o disco persistente padrão zonal.)

   - Disco persistente padrão
   - Disco persistente balanceado
   - Disco persistente SSD

   Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte `<https://cloud.google.com/compute/docs/disks/>`.

7. Na página **Máquinas Virtuais**, especifique quantas VMs você deseja criar, visualize a especificação detalhada das VMs e, em seguida, selecione **Avançar**. Se você usar grupos de nós de locatário único para catálogos de máquinas, certifique-se de selecionar **apenas** as zonas onde os nós de locatário único reservados estão disponíveis. Consulte Habilitar seleção de zona.

8. Na página **Contas de Computador**, selecione uma conta do Active Directory e, em seguida, selecione **Avançar**.

   - Se você selecionar **Criar novas contas do Active Directory**, selecione um domínio e, em seguida, insira a sequência de caracteres que representa o esquema de nomenclatura

para as contas de computador de VM provisionadas criadas no Active Directory. O esquema de nomenclatura da conta pode conter de 1 a 64 caracteres e não pode conter espaços em branco, caracteres não ASCII ou caracteres especiais.

- Se você selecionar **Usar contas existentes do Active Directory**, selecione **Procurar** para navegar até as contas de computador do Active Directory existentes para as máquinas selecionadas.

9. Na página **Credenciais de Domínio**, selecione **Inserir credenciais**, digite o nome de usuário e a senha, selecione **Salvar** e, em seguida, selecione **Avançar**.

   - A credencial que você digita deve ter permissões para realizar operações de conta do Active Directory.

10. Na página **Resumo**, confirme as informações, especifique um nome para o catálogo e, em seguida, selecione **Concluir**.

> **Observação:**
>
> A partir da versão 2402, os nomes de catálogo do GCP devem estar em conformidade com estas regras:
>
> - Começar com uma letra minúscula.
> - Inclua apenas letras minúsculas (a-z), números e hífens.
> - Termine com uma letra minúscula ou um número. Ao tentar renomear catálogos GCP existentes que não estão em conformidade com estas regras, mensagens de erro aparecem e o guiam para renomeá-los de acordo com as regras atualizadas.

A criação do catálogo de máquinas pode levar muito tempo para ser concluída. Para verificar se as máquinas são criadas nos grupos de nós de destino, vá para o console do Google Cloud.

### Importar máquinas do Google Cloud criadas manualmente

Você pode *criar uma conexão com o Google Cloud* e, em seguida, *criar um catálogo contendo máquinas do Google Cloud*. Depois, você pode reiniciar manualmente as máquinas do Google Cloud através do Citrix Virtual Apps and Desktops. Com este recurso, você pode:

- Importar máquinas OS multi-sessão do Google Cloud criadas manualmente para um catálogo de máquinas do Citrix Virtual Apps and Desktops.

- Remover máquinas OS multi-sessão do Google Cloud criadas manualmente de um catálogo do Citrix Virtual Apps and Desktops.
- Usar os recursos de gerenciamento de energia existentes do Citrix Virtual Apps and Desktops para gerenciar o consumo de energia de máquinas OS multi-sessão do Google Cloud Windows. Por exemplo, defina um agendamento de reinício para essas máquinas.

Essa funcionalidade não exige alterações em um fluxo de trabalho de provisionamento existente do Citrix Virtual Apps and Desktops, nem a remoção de qualquer recurso existente. Recomendamos que você use o MCS para provisionar máquinas no Web Studio em vez de importar máquinas do Google Cloud criadas manualmente.

### Nuvem Privada Virtual Compartilhada

Nuvens Privadas Virtuais Compartilhadas (VPCs) compreendem um projeto host, a partir do qual as sub-redes compartilhadas são disponibilizadas, e um ou mais projetos de serviço que usam o recurso. As VPCs Compartilhadas são opções desejáveis para instalações maiores porque fornecem controle centralizado, uso e administração de recursos corporativos compartilhados da nuvem do Google. Para mais informações, consulte o site de Documentação do Google.

Com este recurso, o Machine Creation Services (MCS) oferece suporte ao provisionamento e gerenciamento de catálogos de máquinas implantados em VPCs Compartilhadas. Este suporte, que é funcionalmente equivalente ao suporte atualmente fornecido em VPCs locais, difere em duas áreas:

1. Você deve conceder permissões extras à Conta de Serviço usada para criar a Conexão de Host. Este processo permite que o MCS acesse e use Recursos de VPC Compartilhada.
2. Você deve criar duas regras de firewall, uma para entrada e outra para saída. Essas regras de firewall são usadas durante o processo de masterização da imagem.

#### Novas permissões necessárias

Uma conta de serviço do Google Cloud com permissões específicas é necessária ao criar a conexão do host. Essas permissões adicionais devem ser concedidas a quaisquer contas de serviço usadas para criar conexões de host baseadas em VPC Compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas para o Citrix Virtual Apps and Desktops. Elas são usadas para facilitar a implementação de VPCs locais. Com as VPCs Compartilhadas, essas permissões adicionais permitem o acesso a outros recursos de VPC compartilhados.

> Um máximo de quatro permissões extras devem ser concedidas à conta de serviço associada à conexão do host para suportar o VPC Compartilhado:

1. **compute.firewalls.list** - Esta permissão é obrigatória. Ela permite que o MCS recupere a lista de regras de firewall presentes no VPC Compartilhado.
2. **compute.networks.list** - Esta permissão é obrigatória. Ela permite que o MCS identifique as redes VPC Compartilhadas disponíveis para a conta de serviço.
3. **compute.subnetworks.list** – Esta permissão é opcional, dependendo de como você usa os VPCs. Ela permite que o MCS identifique as sub-redes dentro dos VPCs Compartilhados visíveis. Esta permissão já é exigida ao usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.
4. **compute.subnetworks.use** - Esta permissão é opcional, dependendo de como você usa os VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionados. Esta permissão já é exigida para usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.

Ao usar essas permissões, considere que existem diferentes abordagens com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão em nível de projeto:
  - Permite acesso a todos os VPCs Compartilhados dentro do projeto host.
  - Requer que as permissões #3 e #4 sejam atribuídas à conta de serviço.
- Permissão em nível de sub-rede:
  - Permite acesso a sub-redes específicas dentro do VPC Compartilhado.
  - As permissões #3 e #4 são intrínsecas à atribuição no nível da sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que melhor se adapta às suas necessidades organizacionais e padrões de segurança.

> **Dica:**

> Para obter mais informações sobre as diferenças entre permissões no nível do projeto e no nível da sub-rede, consulte a documentação do Google Cloud.

### Regras de Firewall

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como o disco do sistema da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impede todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total; uma para tráfego de entrada e outra para tráfego de saída. Ao usar VPCs locais do Google Cloud, o MCS cria esse firewall na rede local e o aplica à máquina para masterização. Após a conclusão da masterização, a regra de firewall é removida da imagem.

Recomendamos manter o número de novas permissões necessárias para usar VPCs Compartilhadas no mínimo. As VPCs Compartilhadas são recursos corporativos de nível superior e geralmente possuem protocolos de segurança mais rígidos em vigor. Por esse motivo, crie um par de regras de firewall no projeto host nos recursos da VPC compartilhada, uma para entrada e outra para saída. Atribua a mais alta prioridade a elas. Aplique uma nova tag de destino a cada uma dessas regras, usando o seguinte valor:

```
citrix-provisioning-quarantine-firewall
```

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura por regras de firewall que contenham esta tag de destino. Em seguida, ele examina as regras quanto à correção e as aplica à máquina usada para preparar a imagem mestre para o catálogo. Se as regras de firewall não forem encontradas, ou se as regras forem encontradas, mas as regras ou suas prioridades estiverem incorretas, uma mensagem semelhante à seguinte aparecerá:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

### Configurando a VPC compartilhada

Antes de adicionar a VPC Compartilhada como uma conexão de host no Web Studio, conclua as seguintes etapas para adicionar contas de serviço do projeto no qual você pretende provisionar:

1. Crie uma função IAM.
2. Adicione a conta de serviço usada para criar uma conexão de host CVAD à função IAM do projeto host da VPC Compartilhada.
3. Adicione a conta de serviço do Cloud Build do projeto no qual você pretende provisionar à função IAM do projeto host da VPC Compartilhada.

4. Criar regras de firewall.

### CRIAR UMA FUNÇÃO IAM

Determine o nível de acesso da função — *acesso no nível do projeto* ou um modelo mais restrito usando *acesso no nível da sub-rede*.

**Acesso em nível de projeto para função IAM**. Para a função IAM em nível de projeto, inclua as seguintes permissões:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função IAM em nível de projeto:

1. No console do Google Cloud, navegar até **IAM e administrador > Funções**.
2. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
3. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

**Função IAM em nível de sub-rede**. Esta função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` após selecionar **CRIAR FUNÇÃO**. Para este nível de acesso IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função IAM em nível de sub-rede:

1. No console do Google Cloud, navegar até **Rede VPC** > **VPC compartilhada**. A página **VPC compartilhada** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.
2. Na página **VPC Compartilhada**, selecione a sub-rede que você deseja acessar.
3. No canto superior direito, selecione **ADICIONAR MEMBRO** para adicionar uma conta de serviço.

4. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar um papel** e, em seguida, **Usuário da Rede de Computação**.
    c. Selecione **SALVAR**.
5. No console do Google Cloud, navegar para **IAM e Administrador** > **Funções**.
6. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
7. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

### ADICIONAR UMA CONTA DE SERVIÇO À FUNÇÃO IAM DO PROJETO HOST

Após criar uma função IAM, siga as etapas abaixo para adicionar uma conta de serviço para o projeto host:

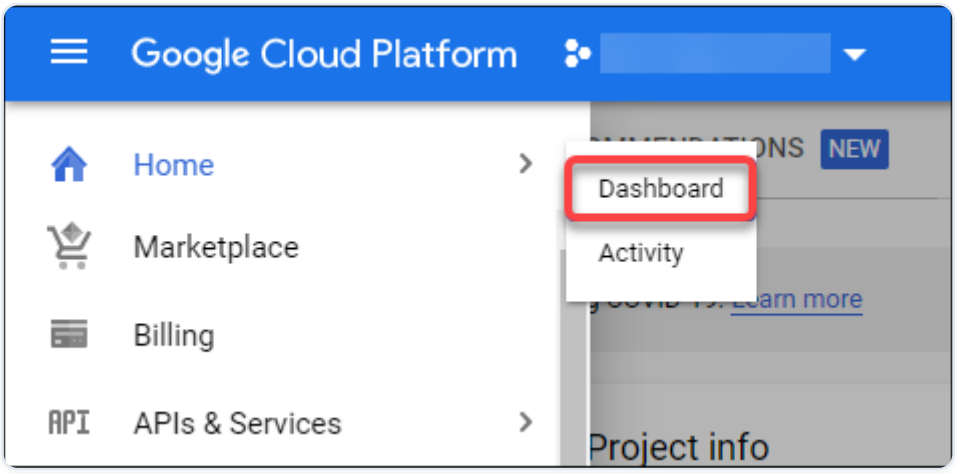
1. No console do Google Cloud, navegar para o projeto host e, em seguida, para **IAM e Administrador > IAM**.
2. Na página **IAM**, selecione **ADICIONAR** para adicionar uma conta de serviço.
3. Na página **Adicionar membros**:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione um campo de função, digite a função IAM que você criou e selecione a função no menu.
    c. Selecione **SALVAR**.

A conta de serviço agora está configurada para o projeto host.

### ADICIONAR A CONTA DE SERVIÇO DE COMPILAÇÃO EM NUVEM AO VPC COMPARTILHADO

Cada assinatura do Google Cloud tem uma conta de serviço que é nomeada após o número de ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar qual é o número de ID do projeto para o seu projeto selecionando **Home** e **Dashboard** no console do Google Cloud:




Encontre o **Número do Projeto** abaixo da área **Informações do Projeto** da tela.

Execute as seguintes etapas para adicionar a conta de serviço do Cloud Build ao VPC Compartilhado:

1. No console do Google Cloud, navegar até o projeto host e depois para **IAM e administrador** > **IAM**.
2. Na página **Permissões**, selecione **ADICIONAR** para adicionar uma conta.
3. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da conta de serviço do Cloud Build e selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar uma função**, digite `Computer Network User` e selecione a função no menu.
    c. Selecione **SALVAR**.

### CRIAR REGRAS DE FIREWALL

Como parte do processo de masterização, o MCS copia a imagem da máquina selecionada e a usa para preparar o disco do sistema da imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que então executa scripts de preparação. Esta VM deve ser executada em um ambiente isolado que proíba todo o tráfego de rede de entrada e saída. Para criar um ambiente isolado, o MCS requer duas regras de firewall *negar tudo*

(uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall no *Projeto Host* da seguinte forma:

1. No console do Google Cloud, navegar até o projeto host e depois para **Rede VPC > Firewall**.
2. Na página **Firewall**, selecione **CRIAR REGRA DE FIREWALL**.
3. Na página **Criar uma regra de firewall**, preencha o seguinte:
    - **Nome**. Digite um nome para a regra.
    - **Rede**. Selecione a rede VPC Compartilhada à qual a regra de firewall de entrada se aplica.
    - **Prioridade**. Quanto menor o valor, maior a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
    - **Direção do tráfego**. Selecione **Entrada**.
    - **Ação na correspondência**. Selecione **Negar**.
    - **Destinos**. Use o padrão, **Tags de destino especificadas**.
    - **Tags de destino**. Digite `citrix-provisioning-quarantine-firewall`.
    - **Filtro de origem**. Use o padrão, **Intervalos de IP**.
    - **Intervalos de IP de origem**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
    - **Protocolos e portas**. Selecione **Negar tudo**.
4. Selecione **CREATE** para criar a regra.
5. Repita as etapas 1 a 4 para criar outra regra. Para **Direção do tráfego**, selecione **Saída**.

#### ADICIONAR UMA CONEXÃO

Adicione uma conexão aos ambientes da nuvem do Google. Consulte Adicionar uma conexão.

### Habilitar seleção de zona

O Citrix Virtual Apps and Desktops oferece suporte à seleção de zona. Com a seleção de zona, você especifica as zonas onde deseja criar VMs. Com a seleção de zona, os administradores podem colocar nós de locatário único em zonas de sua escolha. Para configurar a locação única, você deve concluir o seguinte no Google Cloud:

- Reservar um nó de locatário único do Google Cloud
- Criar a imagem mestre do VDA

### Reservando um nó de locatário único do Google Cloud

Para reservar um nó de locatário único, consulte a documentação do Google Cloud.

> **Importante:**
>
> Um modelo de nó é usado para indicar as características de desempenho do sistema que é reservado no grupo de nós. Essas características incluem o número de vGPUs, a quantidade de memória alocada ao nó e o tipo de máquina usado para máquinas criadas no nó. Para mais informações, consulte a documentação do Google Cloud.

### Criando a imagem mestre do VDA

Para implantar máquinas no nó de locatário único com sucesso, você precisa seguir etapas extras ao criar uma imagem mestre de VM. As instâncias de máquina no Google Cloud têm uma propriedade chamada *rótulos de afinidade de nó*. As instâncias usadas como imagens mestras para catálogos implantados no nó de locatário único exigem um *rótulo de afinidade de nó* que corresponda ao nome do **grupo de nós de destino**. Para conseguir isso, tenha em mente o seguinte:

- Para uma nova instância, defina o rótulo no console do Google Cloud ao criar uma instância. Para obter detalhes, consulte Provisionar uma VM de locatário único.
- Para uma instância existente, defina o rótulo usando a linha de comando **gcloud**. Para obter detalhes, consulte Configurar rótulos de afinidade de nó.

> **Observação:**
>
> Se você pretende usar a locação única com uma VPC compartilhada, consulte Virtual Private Cloud Compartilhada.

#### CRIAR UM CATÁLOGO DE MÁQUINAS

Depois de definir o rótulo de afinidade do nó, configure o catálogo de máquinas.

### Chaves de Criptografia Gerenciadas pelo Cliente (CMEK)

Você pode usar Chaves de Criptografia Gerenciadas pelo Cliente (CMEK) para catálogos MCS. Ao usar essa funcionalidade, você atribui a função `CryptoKey Encrypter/Decrypter` do Google Cloud Key Management Service ao Agente de Serviço do Compute Engine. A conta do

Citrix Virtual Apps and Desktops deve ter as permissões corretas no projeto onde a chave está armazenada. Consulte Ajudando a proteger recursos usando chaves do Cloud KMS para obter mais informações.

Seu Agente de Serviço do Compute Engine está no seguinte formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato é diferente da Conta de Serviço do Compute Engine padrão.

> **Observação:**
>
> Esta Conta de Serviço do Compute Engine pode não aparecer na exibição **Permissões de IAM** do Google Console. Nesses casos, use o comando `gcloud` conforme descrito em Ajudando a proteger recursos usando chaves do Cloud KMS.

### Atribuir permissões à conta do Citrix Virtual Apps and Desktops

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões KMS *no nível do projeto* ou permissões KMS *no nível do recurso*. Consulte Permissões e funções para obter mais informações.

#### PERMISSÕES EM NÍVEL DE PROJETO

Uma opção é fornecer à conta do Citrix Virtual Apps and Desktops permissões em nível de projeto para navegar pelos recursos do Cloud KMS. Para fazer isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua esta função personalizada ao seu Citrix Virtual Apps and Desktops. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

#### PERMISSÕES EM NÍVEL DE RECURSO

Para a outra opção, permissões em nível de recurso, no console do Google Cloud, navegue até o `cryptoKey` que você usa para provisionamento MCS. Adicione a conta do Citrix Virtual Apps and Desktops a um conjunto de chaves ou a uma chave que você usa para provisionamento de catálogo.

**Dica:**

Com esta opção, você não pode navegar pelas chaves regionais do seu projeto no inventário porque a conta do Citrix Virtual Apps and Desktops não tem permissões de lista em nível de projeto nos recursos do Cloud KMS. No entanto, você ainda pode provisionar um catálogo usando CMEK especificando o `cryptoKeyId` correto nas propriedades personalizadas `ProvScheme`, descritas abaixo.

### Provisionamento com CMEK usando propriedades personalizadas

Ao criar seu Esquema de Provisionamento via PowerShell, especifique uma propriedade `CryptoKeyId` em `ProvScheme CustomProperties`. Por exemplo:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

O `cryptoKeyId` deve ser especificado no seguinte formato:

`projectId:location:keyRingName:cryptoKeyName`

Por exemplo, se você quiser usar a chave `my-example-key` no anel de chaves `my-example-key-ring` na região `us-east1` e no projeto com ID `my-example-project-1`, suas configurações personalizadas `ProvScheme` seriam semelhantes a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

Todos os discos e imagens provisionados pelo MCS relacionados a este esquema de provisionamento usam esta chave de criptografia gerenciada pelo cliente.

**Dica:**

Se você usar chaves globais, o local das propriedades do cliente deve dizer `global` e não o nome da **região**, que no exemplo acima é **us-east1**. Por exemplo: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`.

### Rotação de chaves gerenciadas pelo cliente

O Google Cloud não oferece suporte à rotação de chaves em discos persistentes ou imagens existentes. Uma vez que uma máquina é provisionada, ela está vinculada à versão da chave em uso no momento em que foi criada. No entanto, uma nova versão da chave pode ser criada e essa nova chave é usada para máquinas recém-provisionadas ou recursos criados quando um catálogo é atualizado com uma nova imagem mestre.

#### CONSIDERAÇÕES IMPORTANTES SOBRE CONJUNTOS DE CHAVES

Os conjuntos de chaves não podem ser renomeados ou excluídos. Além disso, você pode incorrer em cobranças imprevistas ao configurá-los. Ao excluir ou remover um conjunto de chaves, o Google Cloud exibe uma mensagem de erro:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

**Dica:**

Para obter mais informações, consulte Editar ou excluir um conjunto de chaves do console.

### Compatibilidade de acesso uniforme em nível de bucket

O Citrix Virtual Apps and Desktops é compatível com a política de controle de acesso uniforme em nível de bucket no Google Cloud. Essa funcionalidade aumenta o uso da política IAM que concede permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com o controle de acesso uniforme em nível de bucket, o Citrix Virtual Apps and Desktops permite que você use uma lista de controle de acesso (ACL) para controlar o acesso a buckets de armazenamento ou objetos armazenados neles. Consulte Acesso uniforme em nível de bucket para obter informações gerais sobre o acesso uniforme em nível de bucket do Google Cloud. Para obter informações de configuração, consulte Exigir acesso uniforme em nível de bucket.

### Criar um catálogo de máquinas usando PowerShell

Esta seção detalha como você pode criar catálogos usando PowerShell:

- Criar um catálogo com disco de cache de write-back persistente
- Melhorar o desempenho de inicialização com MCSIO
- Criar um catálogo de máquinas usando um perfil de máquina
- Criar um catálogo de máquinas com perfil de máquina como um modelo de instância
- Usar PowerShell para criar um catálogo com VM blindada
- Criar VMs do Windows 11 no nó de locatário único

### Criar um catálogo com disco de cache de write-back persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro PowerShell `New-ProvScheme` `CustomProperties`.

> **Dica:**
>
> Use o parâmetro PowerShell aqui apenas para conexões de hospedagem baseadas em nuvem. Se você quiser provisionar máquinas usando um disco de cache de write-back persistente para uma solução local (por exemplo, XenServer®), o PowerShell não é necessário porque o disco persiste automaticamente.

Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

**Nota:**

Esse comportamento se aplica tanto ao Azure quanto ao GCP, onde o disco de cache de write-back MCSIO padrão é excluído e recriado durante o ciclo de energia. Você pode optar por manter o disco para evitar a exclusão e recriação do disco de cache de write-back MCSIO.

Definir a propriedade `PersistWBC` como `true` não exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina da interface de gerenciamento.

Definir a propriedade `PersistWBC` como `false` exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina da interface de gerenciamento.

**Nota:**

Se a propriedade `PersistWBC` for omitida, a propriedade assume o padrão `false` e o cache de write-back é excluído quando a máquina é desligada da interface de gerenciamento.

Por exemplo, usando o parâmetro CustomProperties para definir `PersistWBC` como `true`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

**Nota:**

A propriedade `PersistWBC` só pode ser definida usando o cmdlet PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como `true`:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
```

```
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

### Melhorar o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO está habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```
```

Para ativar esse recurso, defina a propriedade personalizada `PersistOSDisk` como `true`. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

### Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS), você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Quando o parâmetro `MachineProfile` não é usado, as propriedades de hardware são capturadas da VM da imagem mestre ou do snapshot. Algumas propriedades que você define explicitamente, por exemplo, `StorageType`, `CatalogZones` e `CryptoKeyIs`, são ignoradas do perfil da máquina.

- Para criar um catálogo com um perfil de máquina, use o comando `New-ProvScheme`. Por exemplo, `New-ProvScheme –MachineProfile "path to VM"`. Se você não especificar o parâmetro `MachineProfile`, as propriedades de hardware serão capturadas da VM da imagem mestre.
- Para atualizar um catálogo com um novo perfil de máquina, use o comando `Set-ProvScheme`. Por exemplo, `Set-ProvScheme –MachineProfile "path to new VM"`. Este comando não altera o perfil de máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.
- Você também pode atualizar a imagem mestre, no entanto, ao atualizar a imagem mestre, as propriedades de hardware não são atualizadas. Se você quiser atualizar as propriedades de hardware, deve atualizar o perfil da máquina usando o comando `Set-ProvScheme`. Essas alterações serão aplicadas apenas às novas máquinas no catálogo. Para atualizar as propriedades de hardware de uma máquina existente, você pode usar o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

  > **Nota:**
  >
  > - `StartsNow` indica que a hora de início agendada é a hora atual.
  > - `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

### Criar um catálogo de máquinas com perfil de máquina como um modelo de instância

Você pode selecionar um modelo de instância do GCP como entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP e, portanto, são muito econômicos.

### Criar um novo catálogo de máquinas com perfil de máquina como um modelo de instância

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Encontre um modelo de instância em seu projeto GCP usando o seguinte comando:

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. Crie um novo catálogo de máquinas com perfil de máquina como um modelo de instância usando o comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   Para obter mais informações sobre o comando New-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Conclua a criação do catálogo de máquinas usando comandos PowerShell. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância

As etapas detalhadas para alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância são:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
```

```
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Para obter informações sobre o comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Usar PowerShell para criar um catálogo com VM blindada

Você pode criar um catálogo de máquinas MCS com propriedades de VM blindada. Uma máquina virtual blindada é reforçada por um conjunto de controles de segurança que fornecem integridade verificável de suas instâncias do Compute Engine, usando recursos avançados de segurança da plataforma, como inicialização segura, um módulo de plataforma confiável virtual, firmware UEFI e monitoramento de integridade.

O MCS oferece suporte à criação do catálogo usando o fluxo de trabalho de perfil de máquina. Se você usar o fluxo de trabalho de perfil de máquina, deverá habilitar as propriedades de VM blindada de uma instância de VM. Você pode então usar esta instância de VM como entrada de perfil de máquina.

Para criar um catálogo de máquinas MCS com VM blindada usando o fluxo de trabalho de perfil de máquina.

1. Habilite as opções de VM blindada de uma instância de VM no console do Google Cloud. Consulte Início rápido: Habilitar opções de VM blindada.
2. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina usando a instância de VM.
    a. Abra uma janela do PowerShell.
    b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
    c. Crie um pool de identidades se ainda não tiver sido criado.
    d. Execute o comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
```

```
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. Conclua a criação do catálogo de máquinas.

Para atualizar o catálogo de máquinas com um novo perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

Para aplicar a alteração feita em `Set-ProvScheme` às VMs existentes, execute o comando `Set-ProvVMUpdateTimeWindow`.

1. Execute o comando `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. Reinicie as VMs.

### Crie VMs do Windows 11 no nó de locatário único

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

As principais etapas para criar VMs do Windows 11 no nó de locatário único são:

1. Configure os ambientes de virtualização do Google Cloud. Para obter informações, consulte Ambientes do Google Cloud.
2. Instale o VDA. Consulte Instalar VDAs.
3. Crie uma conexão com os ambientes do Google Cloud. Para obter informações, consulte Conexão com ambientes do Google Cloud.
4. Crie uma imagem mestre do Windows 11 Bring Your Own License (BYOL) e importe a imagem para o Google Cloud. Consulte Criar uma imagem mestre BYOL do Windows 11.

5. Crie a origem do perfil da máquina: Provisione a VM no nó de locatário único e habilite o vTPM do perfil da máquina de origem. Consulte Provisionar VM no nó de locatário único.
6. Crie um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11 habilitada com vTPM. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único. Consulte Criar um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11.

### Criar uma imagem mestre BYOL do Windows 11

Existem duas opções para criar uma imagem mestre BYOL do Windows 11 e importar a imagem mestre para o Google Cloud:

- Usar as Ferramentas de Compilação do Google Cloud
- Criar a imagem mestre em qualquer outro hipervisor

#### USAR AS FERRAMENTAS DE COMPILAÇÃO DO GOOGLE CLOUD

1. Carregue os arquivos ISO do Windows 11, GCP SDK, .NET framework e instalador do PowerShell para o bucket de armazenamento do GCP.
2. Forneça o local do arquivo no arquivo `.yaml` de compilação na nuvem como parâmetro.
3. Execute o seguinte Cloud Build a partir da linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

Para obter informações completas, consulte Criar imagens BYOL personalizadas do Windows.

#### CRIE A IMAGEM MESTRE EM QUALQUER OUTRO HIPERVISOR

1. Crie a imagem mestre do Windows 11 usando qualquer outro hipervisor.
2. Exporte a imagem mestre em formato OVF para a máquina local.

3. Faça upload dos arquivos OVF para o bucket de armazenamento do GCP usando a CLI gcloud local.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. Execute o seguinte Cloud Build na linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

### Provisionar VM em nó de locatário único

Use nós de locatário único para manter suas VMs fisicamente separadas de VMs em outros projetos, ou para agrupar suas VMs no mesmo hardware de host. Para obter informações sobre o nó de locatário único, consulte o documento do GCP Visão geral da locação única.

Para provisionar uma VM (origem do perfil da máquina) no nó de locatário único, consulte o documento do GCP Provisionar VMs em nós de locatário único.

> **Nota:**
>
> - Selecione o mesmo tipo de instância e região que o grupo de nós.
> - Habilite o vTPM na seção VM Blindada. Para obter mais informações, consulte Início rápido: Habilitar opções de VM Blindada.
> - Desative o Bitlocker na VM de origem.

### Criar um catálogo de máquinas MCS usando a origem do perfil de máquina do Windows 11

Você pode criar um catálogo de máquinas MCS para criar VMs do Windows 11 usando o Web Studio ou comandos do PowerShell.

**Nota:**

- Para a imagem mestre, selecione o Snapshot ou a VM do Windows 11.
- Para a origem do perfil da máquina, selecione a VM do Windows 11 como perfil da máquina. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único.

Para obter informações sobre como usar o Web Studio, consulte Criar um catálogo de máquinas usando o Web Studio.

Para obter informações sobre comandos do PowerShell, consulte Criar um catálogo de máquinas usando um perfil de máquina

Depois de criar o catálogo e ligar as VMs, você pode ver as VMs do Windows 11 sendo executadas no nó de locatário único no console do Google Cloud.

### Google Cloud Marketplace

Você pode navegar e selecionar imagens oferecidas pela Citrix no **Google Cloud Marketplace** para criar catálogos de máquinas. Atualmente, o MCS oferece suporte apenas ao fluxo de trabalho de perfil de máquina para este recurso.

Para pesquisar o produto VM Citrix VDA através do Google Cloud Marketplace, acesse https://console.cloud.google.com/marketplace.

Você pode usar uma imagem personalizada ou uma imagem Citrix ready® no **Google Cloud Marketplace** para atualizar uma imagem de um catálogo de máquinas.

**Nota:**

Se o perfil da máquina não contiver informações de tipo de armazenamento, o valor será derivado das propriedades personalizadas.

> As imagens suportadas do Google Cloud Marketplace são:

- Windows 2019 Single Session
- Windows 2019 Multissessão
- Ubuntu

Exemplo de uso de uma imagem pronta para Citrix como fonte para criar um catálogo de máquinas:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Google Cloud Platform

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas

## Criar um catálogo de máquinas HPE Moonshot

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes HPE Moonshot.

> **Observação:**

- Criar uma conexão com o HPE Moonshot
- Certifique-se de ter um ou mais nós HPE Moonshot disponíveis e instale VDAs nesses nós.
- Para obter informações sobre como criar a imagem inicial do cartucho HPE Moonshot, consulte o Guia do Usuário de Implantação de SO no Moonshot.

Você pode criar um catálogo de máquinas HPE Moonshot usando:

- Web Studio
- Comandos PowerShell

### Criar um catálogo de máquinas usando o Web Studio

No assistente de **Configuração do Catálogo de Máquinas**:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e **Outro serviço ou tecnologia**.
3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode fazer uma das seguintes opções:
   - Clique em **Adicionar Máquinas** para adicionar máquinas manualmente. A janela **Selecionar VMs** é exibida. Expanda a conexão do chassi HPE Moonshot que você criou anteriormente e selecione os nós (VMs) que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.
   - Clique em **Adicionar Arquivo CSV** para adicionar máquinas em massa. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

As páginas **Escopos** e **Resumo** não contêm informações específicas do HPE Moonshot.

### Criar um catálogo de máquinas usando comandos PowerShell

Execute os comandos PowerShell `New-BrokerCatalog` e `New-BrokerMachine` para criar um catálogo de broker e importar máquinas para o catálogo de broker.

Por exemplo:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo HPE Moonshot

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com HPE Moonshot
- Criar catálogos de máquinas

## Criar um catálogo do Microsoft Azure

> **Nota:**

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

> (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

**Nota:**

Antes de criar um catálogo do Microsoft Azure, você precisa concluir a criação de uma conexão com o Microsoft Azure. Consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-azure-resource-manager.html).

### Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio
- Criar um catálogo de máquinas usando o PowerShell

#### Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio

Uma imagem pode ser um disco, um instantâneo ou uma versão de imagem de uma definição de imagem dentro da Galeria de Computação do Azure que é usada para criar as VMs em um catálogo de máquinas. Antes de criar o catálogo de máquinas, crie uma imagem no Azure Resource Manager. Para informações gerais sobre imagens, consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html).

**Nota:**

O suporte para usar uma imagem mestre de uma região diferente da configurada na conexão do host foi descontinuado. Use a Galeria de Computação do Azure para replicar a imagem mestre para a região desejada.

Ao criar um catálogo de máquinas MCS, uma VM temporária é criada com base na VM original para executar tarefas de preparação, como habilitar DHCP e rearmar a licença. Essa VM temporária é chamada de VM de preparação. O nome dessa VM de preparação segue o formato **Preparati-84x9n**, onde os últimos cinco caracteres são gerados aleatoriamente para evitar duplicação. A convenção de nomenclatura para essa VM de preparação é fixa e não pode ser personalizada. Após a conclusão das tarefas de preparação, a VM de preparação é destruída.

Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. O grupo de segurança de rede é criado automaticamente uma vez por catálogo. O nome do grupo de segurança de rede é `Citrix-Deny-All-a3pgu-GUID`, onde GUID é gerado aleatoriamente. Por exemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

No assistente de criação de catálogo de máquinas:

- As páginas **Tipo de Máquina** e **Gerenciamento de Máquinas** não contêm informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.
- Na página **Imagem**, escolha uma imagem que você deseja usar como modelo para criar máquinas neste catálogo.

  Se você selecionar **Imagem mestre** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e siga estas etapas para selecionar uma imagem mestre conforme necessário:

  a. (Aplicável apenas a conexões configuradas com imagens compartilhadas dentro ou entre locatários) Selecione uma assinatura onde a imagem reside.
  b. Selecione um grupo de recursos.
  c. navegar para o VHD do Azure, a Galeria de Computação do Azure ou a versão da imagem do Azure. Adicione uma nota para a imagem selecionada, se necessário.

  Ao selecionar uma imagem, considere o seguinte:

  - Verifique se um Citrix VDA está instalado na imagem.
  - Se você selecionar um VHD anexado a uma VM, deverá desligar a VM antes de prosseguir para a próxima etapa.

> **Nota:**
>
> - A assinatura correspondente à conexão (host) que criou as máquinas no catálogo é indicada com um ponto verde. As outras assinaturas são aquelas que têm a Azure Compute Gallery compartilhada com essa assinatura. Nessas assinaturas, apenas galerias compartilhadas são mostradas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens dentro de um locatário (entre assinaturas) e Compartilhar imagens entre locatários.

- O uso de um perfil de máquina com inicialização confiável como **Tipo de Segurança** é obrigatório ao selecionar uma imagem ou instantâneo que tenha a inicialização confiável habilitada. Você pode então habilitar ou desabilitar o SecureBoot e o vTPM especificando seus valores no perfil da máquina. A Inicialização Confiável não é suportada para a Galeria de Imagens Compartilhadas. Para obter informações sobre a inicialização confiável do Azure, consulte `<https://docs.microsoft.com/pt-br/azure/virtual-machines/trusted-launch>`.
- Você pode criar um esquema de provisionamento usando disco de SO efêmero no Windows com inicialização confiável. Ao selecionar uma imagem com inicialização confiável, você deve selecionar um perfil de máquina com inicialização confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
- Quando a replicação da imagem estiver em andamento, você pode prosseguir e selecionar a imagem como imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode levar mais tempo para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída em uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo falhará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.
- Ao selecionar uma imagem mestre para catálogos de máquinas no Azure, o MCS identifica o tipo de SO com base na imagem mestre e no perfil de máquina selecionados. Se o MCS não conseguir identificá-lo, selecione o tipo de SO que corresponde à imagem mestre.
- Você pode provisionar um catálogo de VMs Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem mais antiga que não tenha informações de geração é uma imagem Gen1.

Se você selecionar **Imagem preparada** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e selecione uma imagem preparada conforme necessário.

Para garantir a criação bem-sucedida da VM, verifique se a imagem tem o Citrix VDA 2311 ou posterior instalado e se o MCSIO está presente no VDA.

Depois de selecionar uma imagem, a caixa de seleção **Usar um perfil de máquina (obrigatório para o Azure Active Directory)** é selecionada automaticamente. Clique em **Selecionar um perfil de máquina** para procurar uma VM ou uma especificação de modelo ARM em uma lista de grupos de recursos. As VMs no catálogo podem herdar configurações do perfil de máquina selecionado.

Valide a especificação do modelo ARM para garantir que ela possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Existem duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Avançar**. Mensagens de erro aparecerão se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Exemplos de configurações que as VMs podem herdar de um perfil de máquina incluem:

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

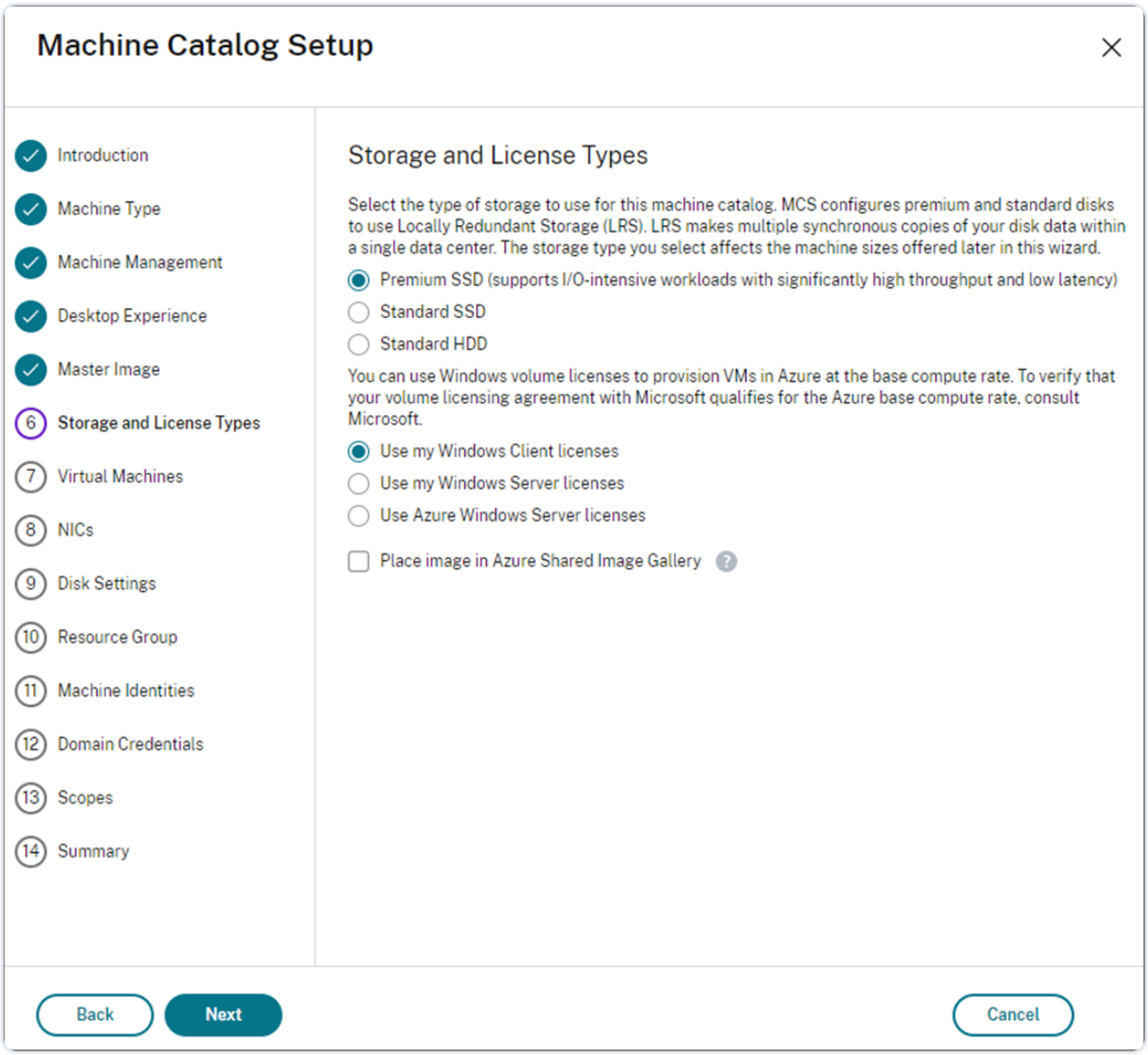
Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Catálogos de Máquinas**, selecione o catálogo para visualizar seus detalhes no painel inferior. Em seguida, clique na guia **Propriedades do Modelo** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **Ver tudo**.

Se você deseja que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts dedicado** e, em seguida, selecione um grupo de hosts na lista. Um grupo de hosts é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço que fornece servidores físicos que hospedam uma ou mais VMs. Seu servidor é dedicado à sua assinatura do Azure, não compartilhado com outros assinantes. Ao usar um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em

execução nesse host. Esse recurso é adequado para cenários em que você deve atender a requisitos regulatórios ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

> **Importante:**
>
> - Somente os grupos de hosts que têm o posicionamento automático do Azure habilitado são exibidos.
> - O uso de um grupo de hosts altera a página **Máquinas Virtuais** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são exibidos nessa página. Além disso, as Zonas de Disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Tipos de Armazenamento e Licença** aparece somente quando você usa uma imagem do Azure Resource Manager.




Você tem os seguintes tipos de armazenamento para usar no catálogo de máquinas:

- **SSD Premium**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência, adequada para VMs com cargas de trabalho intensivas em E/S.
- **SSD Standard**. Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
- **Standard HDD**. Oferece uma opção de armazenamento em disco confiável e de baixo custo, adequada para VMs que executam cargas de trabalho insensíveis à latência.
- **Disco de SO efêmero do Azure**. Oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Alternativamente, você pode usar o PowerShell para criar máquinas que usam discos de SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Esteja ciente das seguintes considerações ao usar um disco de SO efêmero:

- O disco de SO efêmero do Azure e o MCS I/O não podem ser habilitados ao mesmo tempo.
- Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
- Você não pode usar a opção **Manter VM e disco do sistema durante ciclos de energia** oferecida posteriormente no assistente.

> **Nota:**
>
> O disco de identidade é sempre criado usando SSD Standard, independentemente do tipo de armazenamento escolhido.

> 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 Redundante Localmente (LRS). O LRS faz várias cópias síncronas dos dados do seu 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/pt-br/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/pt-br/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/pt-br/azure/storage/common/storage-redundancy/>`

Selecione se deseja usar licenças Windows existentes ou licenças Linux.

- Licenças Windows: O uso de licenças Windows juntamente com imagens Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs Windows no Azure a um custo reduzido. Existem dois tipos de licenças:
  - **Licença do Windows Server**. Permite que você use suas licenças do Windows Server ou do Azure Windows Server, permitindo que você use os Benefícios Híbridos do Azure. Para obter detalhes, consulte `<https://azure.microsoft.com/pt-br/`

`pricing/hybrid-benefit/>`. O Benefício Híbrido do Azure reduz o custo de execução de VMs no Azure para a taxa de computação base, dispensando o custo de licenças extras do Windows Server da galeria do Azure.

- **Licença de Cliente Windows**. Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de Acesso para Cliente e Licenças de Gerenciamento.

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows_Server**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`.
- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows_Client**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`.

Alternativamente, você pode usar o `Get-Provscheme` PowerShell SDK para fazer a verificação. Por exemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre este cmdlet, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`.

- Licenças Linux: Com as licenças Linux bring-your-own-subscription (BYOS), você não precisa pagar pelo software. A cobrança do BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:
  - **RHEL_BYOS**: Para usar o tipo RHEL_BYOS com sucesso, habilite o Red Hat Cloud Access em sua assinatura do Azure.
  - **SLES_BYOS**: As versões BYOS do SLES incluem suporte da SUSE.

  Você pode definir o valor de LicenseType para as opções do Linux em `New-ProvScheme` e `Set-ProvScheme`.

  Exemplo de configuração de LicenseType para RHEL_BYOS em `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

Exemplo de configuração de LicenseType para SLES_BYOS em `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

**Observação:**

Se o valor `LicenseType` estiver vazio, os valores padrão serão Licença do Azure Windows Server ou Licença do Azure Linux, dependendo do valor de OsType.

Exemplo de como definir LicenseType como vazio:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
```

```
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

Consulte os seguintes documentos para entender os tipos de licença e seus benefícios:

- `<https://docs.microsoft.com/pt-br/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/pt-br/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

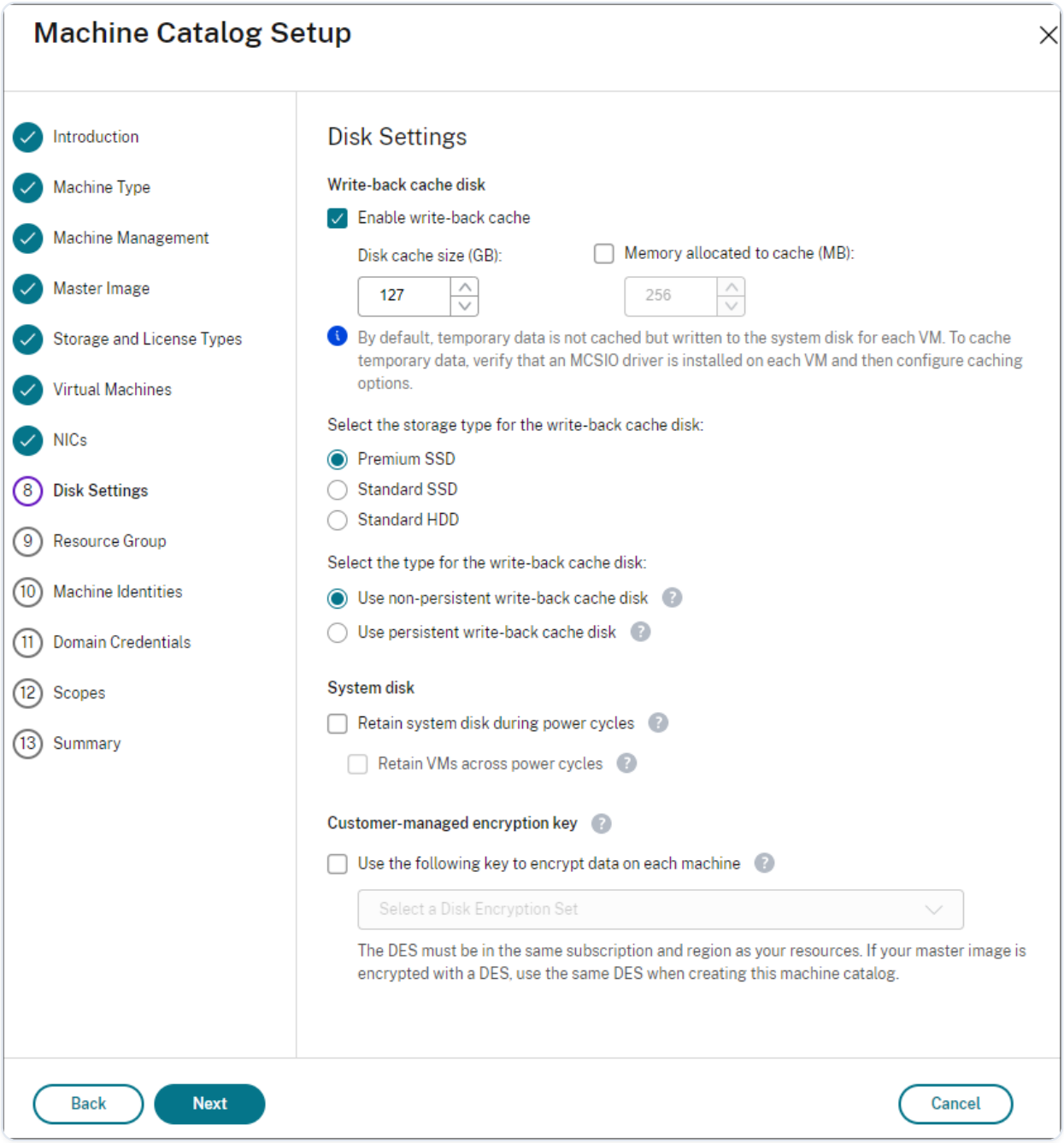
A Galeria de Computação do Azure (anteriormente Galeria de Imagens Compartilhadas do Azure) é um repositório para gerenciar e compartilhar imagens. Ela permite que você disponibilize suas imagens em toda a sua organização. Recomendamos que você armazene uma imagem na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos do SO VDA. Depois de selecionar **Colocar imagem preparada na Galeria de Computação do Azure**, a seção **Configurações da Galeria de Computação do Azure** aparece, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

- **Proporção de máquinas virtuais para réplicas de imagem**. Permite que você especifique a proporção de máquinas virtuais para réplicas de imagem que você deseja que o Azure mantenha. Por padrão, o Azure mantém uma única réplica de imagem para cada 40 máquinas não persistentes. Para máquinas persistentes, esse número padrão é 1.000.
- **Contagem máxima de réplicas**. Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 10.

> **Observação:**
>
> Uma galeria é criada no ACG para armazenar a imagem. Esta galeria é acessível apenas ao MCS para criação de VM e não aparece na página **Selecionar uma imagem**.

- Na página **Máquinas Virtuais**, indique quantas VMs você deseja criar. Você deve especificar pelo menos uma e selecionar um tamanho de máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.

- A página **NICs** não contém informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.
- Na página **Configurações de Disco**, escolha se deseja habilitar o cache de write-back. Com o recurso de otimização de armazenamento do MCS habilitado, você pode configurar as seguintes configurações ao criar um catálogo. Essas configurações se aplicam a ambientes Azure e GCP.




Após habilitar o cache de write-back, você pode fazer o seguinte:

  - Configure o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.

- Selecione o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:
  - SSD Premium
  - SSD Standard
  - HDD Standard
- Escolha se deseja que o disco de cache de write-back persista para as VMs provisionadas. Selecione **Habilitar cache de write-back** para disponibilizar as opções. Por padrão, **Usar disco de cache de write-back não persistente** é selecionado.
- Selecione o tipo para o disco de cache de write-back.
  - **Usar disco de cache de write-back não persistente**. Se selecionado, o disco de cache de write-back é excluído durante os ciclos de energia. Quaisquer dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache de write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Propriedades do Modelo**. Se o disco temporário for usado, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Sim (usando o disco temporário da VM)**. Caso contrário, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Não (não usando o disco temporário da VM)**.
  - **Usar disco de cache de write-back persistente**. Se selecionado, o disco de cache de write-back persiste para as VMs provisionadas. Habilitar a opção aumenta seus custos de armazenamento.
- Escolha se deseja reter VMs e discos de sistema para VDAs durante os ciclos de energia.

  **Reter VM e disco do sistema durante ciclos de energia**. Disponível quando você selecionou **Habilitar cache de write-back**. Por padrão, as VMs e os discos do sistema são excluídos no desligamento e recriados na inicialização. Se você deseja reduzir os tempos de reinicialização da VM, selecione esta opção. Lembre-se de que habilitar esta opção também aumenta os custos de armazenamento.
- Escolha se deseja habilitar **Economia de custos de armazenamento**. Se habilitado, economize custos de armazenamento rebaixando o disco de armazenamento para HDD Padrão quando a VM for desligada. A VM retorna às suas configurações originais na reinicialização. A opção se aplica a discos de armazenamento e de cache de write-back.

Alternativamente, você também pode usar o PowerShell. Consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

> **Observação:**
>
> A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie alterações no tipo de armazenamento no futuro. Para obter mais informações, consulte este artigo da Microsoft.

- Escolha se deseja criptografar dados nas máquinas provisionadas no catálogo. A criptografia do lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia no nível do disco gerenciado e proteger os dados nas máquinas do catálogo. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

- Na página **Grupo de Recursos**, escolha se deseja criar grupos de recursos ou usar grupos existentes.
  - Se você optar por criar grupos de recursos, selecione **Avançar**.
  - Se você optar por usar grupos de recursos existentes, selecione os grupos na lista **Grupos de Recursos de Provisionamento Disponíveis**. **Lembre-se**: Selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Uma mensagem aparece se você escolher poucos. Você pode querer selecionar mais do que o mínimo necessário se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que ele é criado.

  Para obter mais informações, consulte Grupos de recursos do Azure.
- Na página **Identidades da Máquina**, escolha um tipo de identidade e configure as identidades para as máquinas neste catálogo. Se você selecionar as VMs como **Unidas ao Azure Active Directory**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:

  a. No campo **Tipo de identidade**, selecione **Unido ao Azure Active Directory**. A opção **Grupo de segurança do Azure AD (opcional)** aparece.

  b. Clique em **Grupo de segurança do Azure AD: Criar novo**.

  c. Insira um nome de grupo e depois clique em **Criar**.

d. Siga as instruções na tela para fazer login no Azure. Se o nome do grupo não existir no Azure, um ícone verde aparecerá. Caso contrário, uma mensagem de erro aparecerá solicitando que você insira um novo nome.

e. Insira o esquema de nomenclatura da conta de máquina para as VMs.

Após a criação do catálogo, o Citrix Virtual Apps and Desktops™ acessa o Azure em seu nome e cria o grupo de segurança e uma regra de associação dinâmica para o grupo. Com base na regra, as VMs com o esquema de nomenclatura especificado neste catálogo são adicionadas automaticamente ao grupo de segurança.

Adicionar VMs com um esquema de nomenclatura diferente a este catálogo exige que você faça login no Azure. O Citrix Virtual Apps and Desktops pode então acessar o Azure e criar uma regra de associação dinâmica com base no novo esquema de nomenclatura.

Ao excluir este catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.

- As páginas **Credenciais de Domínio** e **Resumo** não contêm informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.

Conclua o assistente.

### Condições para que o disco temporário do Azure seja elegível para disco de cache de write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem satisfeitas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.
- O tamanho da VM do Azure escolhido deve incluir um disco temporário.
- O disco do SO efêmero não precisa ser habilitado.
- Aceitar colocar o arquivo de cache de write-back no disco temporário do Azure.
- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco de cache de write-back + espaço reservado para arquivo de paginação + 1 GB de espaço de buffer).

### Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back ao criar um catálogo de máquinas.

| CENÁRIO | RESULTADO |
| --- | --- |
| Todas as condições para usar o disco temporário para cache de write-back são satisfeitas. | O arquivo WBC `mcsdif.vhdx` é colocado no disco temporário. |
| O disco temporário tem espaço insuficiente para uso do cache de write-back. | Um disco VHD `MCSWCDisk` é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco. |
| O disco temporário tem espaço suficiente para uso do cache de write-back, mas `UseTempDiskForWBC` está definido como **false**. | Um disco VHD `MCSWCDisk` é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco. |

### Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la no Web Studio e em comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Vá para o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a VM e a interface de rede. No menu **…** na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para provisionamento de catálogo.
3. Clique em **Adicionar à biblioteca** para modificar a especificação de modelo mais tarde.
4. Na página **Importando modelo**, insira as informações necessárias, como **Nome**, **Assinatura**, **Grupo de Recursos**, **Localização** e **Versão**. Clique em **Avançar: 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:

   ```
   "dependsOn": [

   "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"

   ],
   ```

6. Crie **Revisar+Criar** e crie a especificação de modelo.

7. Na página **Especificações de Modelo**, verifique a especificação de modelo que você acabou de criar. Clique na especificação de modelo. No painel esquerdo, clique em **Versões**.
8. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação de modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação de modelo.

Você pode obter informações sobre a especificação do modelo e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação do modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- Para obter informações sobre a versão da especificação do modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

### Usar especificação de modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou comandos do PowerShell.

- Para o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio
- Para o PowerShell, consulte Usar especificação de modelo na criação ou atualização de um catálogo usando o PowerShell

### Criptografia do lado do servidor do Azure

O Citrix Virtual Apps and Desktops oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados do seu catálogo de máquinas usando sua própria chave de criptografia. Para obter

mais informações, consulte Criptografia do lado do servidor do Armazenamento em Disco do Azure.

Ao usar este recurso para discos gerenciados:

- Para alterar a chave com a qual o disco é criptografado, você altera a chave atual no `DiskEncryptionSet`. Todos os recursos associados a esse `DiskEncryptionSet` mudam para serem criptografados com a nova chave.
- Quando você desativa ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja ativada novamente ou você atribua uma nova chave. Qualquer catálogo que use a chave não pode ser ligado, e você não pode adicionar VMs a ele.

**Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente**

Considere o seguinte ao usar este recurso:

- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Depois de habilitar a chave de criptografia gerenciada pelo cliente, você não poderá desativá-la posteriormente. Se você 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 do 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.
- Discos gerenciados atualmente ou anteriormente criptografados usando o Azure Disk Encryption não podem ser criptografados usando chaves gerenciadas pelo cliente.
- Consulte o site da Microsoft para obter informações sobre as limitações dos conjuntos de criptografia de disco por região.

> **Nota:**

> Consulte Início rápido: Criar um Key Vault usando o portal do Azure para obter informações sobre como configurar a criptografia do lado do servidor do Azure.

### Chave de criptografia gerenciada pelo cliente do Azure

Ao criar um catálogo de máquinas, você pode escolher se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia do lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas do catálogo. Um Conjunto de Criptografia de Disco (DES) representa uma chave gerenciada pelo cliente. Para usar esse recurso, você deve primeiro criar seu DES no Azure. Um DES está no seguinte formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos. Se sua imagem for criptografada com um DES, use o mesmo DES ao criar o catálogo de máquinas. Você não pode alterar o DES depois de criar o catálogo.

Se você criar um catálogo com uma chave de criptografia e, posteriormente, desativar o DES correspondente no Azure, não poderá mais ligar as máquinas no catálogo ou adicionar máquinas a ele.

Consulte Criando um catálogo de máquinas usando chave gerenciada pelo cliente.

### Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta apenas o fluxo de trabalho de perfil de máquina para este recurso. Você pode usar uma VM ou uma especificação de modelo como entrada para um perfil de máquina.

Este método de criptografia não criptografa os dados através do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem através do servidor de armazenamento do Azure. Portanto, este método de criptografia criptografa os dados de ponta a ponta.

**Restrições:**

A criptografia de disco do Azure no host é:

- Não suportada para todos os tamanhos de máquina do Azure
- Incompatível com a criptografia de disco do Azure

Para criar um catálogo de máquinas com capacidade de criptografia no host:

1. Verifique se a assinatura tem o recurso de criptografia no host habilitado ou não. Para fazer isso, consulte `<https://learn.microsoft.com/pt-br/rest/api/resources/features/get?tabs=HTTP/>`. Se não estiver habilitado, você deve habilitar o recurso para a assinatura. Para obter informações sobre como habilitar o recurso para sua assinatura, consulte `<https://learn.microsoft.com/pt-br/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`.
2. Verifique se um tamanho de VM específico do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute um dos seguintes:

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. Crie uma VM ou uma especificação de modelo, como entrada para o perfil da máquina, no portal do Azure com a criptografia no host ativada.

   - Se você quiser criar uma VM, selecione um tamanho de VM que suporte criptografia no host. Depois de criar a VM, a propriedade da VM **Criptografia no host** é habilitada.
   - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `securityProfile`.

4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina, selecionando uma VM ou uma especificação de modelo.

   - Disco do SO / Disco de Dados: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma
   - Disco do SO Efêmero: É criptografado apenas por meio de chave gerenciada pela plataforma
   - Disco de Cache: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma

Você pode criar o catálogo de máquinas usando o Web Studio ou executando comandos 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 de máquina.

Por exemplo: Quando a entrada do perfil da máquina é uma VM, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

Por exemplo: Quando a entrada do perfil da máquina é uma especificação de modelo, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

## Criptografia dupla em disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Quaisquer catálogos criados com esse recurso têm todos os discos criptografados no lado do servidor com chaves gerenciadas pela plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a Chave de Criptografia e os Conjuntos de Criptografia de Disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. Discos de SO e dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

**Nota:**

- Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e comandos do PowerShell. Consulte Criar um catálogo de máquinas com criptografia dupla para comandos do PowerShell.
- Você pode usar o fluxo de trabalho baseado em perfil não-máquina ou o fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
- Se você usar o fluxo de trabalho baseado em perfil não-máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetId` armazenado.
- Se você usar um perfil de máquina, poderá usar uma VM ou especificação de modelo como entrada de perfil de máquina.

**Limitações:**

- A criptografia dupla não é suportada para Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desabilitar uma chave DiskEncryptionSet associada a um catálogo, as VMs do catálogo serão desabilitadas.
- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você pode criar apenas até 50 conjuntos de criptografia de disco por região por assinatura.
- Você não pode atualizar um catálogo de máquinas que já possui 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 desktops aos usuários. Você pode adicionar grupos de recursos do Azure vazios existentes ao criar um catálogo de máquinas MCS, ou ter novos grupos de recursos criados para você. Para obter informações sobre grupos de recursos do Azure, consulte a documentação da Microsoft.

#### Uso do Grupo de Recursos do Azure

Não há limite para o número de máquinas virtuais, discos gerenciados, instantâneos e imagens por Grupo de Recursos do Azure. (O limite de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure foi removido.)

- Ao usar um principal de serviço de escopo total para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar um principal de serviço de escopo restrito para criar um catálogo de máquinas, você deve fornecer um Grupo de Recursos do Azure vazio e pré-criado para o catálogo.

### Discos efêmeros do Azure

Um disco efêmero do Azure permite que você reutilize o disco de cache ou o disco temporário para armazenar o disco do sistema operacional para uma máquina virtual habilitada para Azure. Essa funcionalidade é útil para ambientes Azure que exigem um disco SSD de maior desempenho em vez de um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte Criar um catálogo com discos efêmeros do Azure.

> **Nota:**
>
> Catálogos persistentes não suportam discos de SO efêmeros.
>
> Os discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Imagens Compartilhadas.

#### Armazenando um disco temporário de SO efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM ou em um disco de recurso. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não possui cache ou possui cache insuficiente. Essas VMs têm um disco temporário ou de recurso para armazenar um disco de SO efêmero, como `Ddv4`.

Considere o seguinte:

- Um disco efêmero é armazenado no disco de cache da VM ou no disco temporário (de recurso) da VM. O disco de cache é preferido em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco do SO.
- Para atualizações, uma nova imagem que é maior que o disco de cache, mas menor que o disco temporário, resulta na substituição do disco de SO efêmero pelo disco temporário da VM.

#### Disco efêmero do Azure e otimização de armazenamento do Machine Creation Services (MCS) (MCS I/O)

O disco de SO efêmero do Azure e o MCS I/O não podem ser ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Você não pode criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- Os parâmetros do PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) falham com mensagens de erro apropriadas se você os definir como **true** em `New-ProvScheme` ou `Set-ProvScheme`.
- Para catálogos de máquinas existentes criados com ambas as funcionalidades ativadas, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

### Galeria de Computação do Azure

Use o Azure Compute Gallery (anteriormente Azure Shared Image Gallery) como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação de discos de SO, melhorando os tempos de inicialização e de lançamento de aplicativos para VMs não persistentes. A galeria de imagens compartilhadas contém os três elementos a seguir:

- *Galeria*: As imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de Imagem da Galeria*: Esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- *Versão da Imagem da Galeria*: Cada imagem em uma Galeria de Imagens Compartilhadas pode ter várias versões, e cada versão pode ter várias réplicas em diferentes regiões. Cada réplica é uma cópia completa da imagem publicada.

> **Nota:**
>
> A funcionalidade da Galeria de Imagens Compartilhadas é compatível apenas com discos gerenciados. Não está disponível para catálogos de máquinas legados.

> Para obter mais informações, consulte Visão geral do Azure Compute Gallery.

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 uma imagem da Galeria de Computação do Azure.

### VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que seu desktop virtual seja criptografado na memória e protegido em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto VM quanto a especificação de modelo ARM como entrada de perfil de máquina.

#### Considerações importantes para VMs confidenciais

As considerações importantes para tamanhos de VM suportados e criação de catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM suportados: As VMs Confidenciais suportam os seguintes tamanhos de VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Crie catálogos de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com VMs Confidenciais do Azure usando o Web Studio e comandos do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquinas com VMs Confidenciais do Azure. Você pode usar uma VM ou especificação de modelo como entrada de perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar habilitadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:
    - **VMGuestStateOnly**: VM confidencial com apenas o estado do convidado da VM criptografado
    - **DiskWithVMGuestState**: VM confidencial com disco do SO e estado do convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco do SO normal quanto o efêmero podem ser criptografados.

- Você pode obter informações de VM confidenciais de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM, usando o parâmetro AdditionalData. Por exemplo:

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  Os campos de dados adicionais são:

  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  Para obter a propriedade de computação confidencial de um tamanho de máquina, execute o seguinte comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  O campo de dados adicionais é `ConfidentialComputingType`.

- Você não pode alterar a imagem mestre ou o perfil da máquina de tipo de segurança confidencial para não confidencial, ou de não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

**Preparar imagens mestre e perfis de máquina**

Antes de criar um conjunto de VMs confidenciais, siga estas etapas para preparar uma imagem mestre e um perfil de máquina para elas:

1. No portal do Azure, crie uma VM confidencial com configurações específicas, como:
   - **Tipo de Segurança**: Máquinas virtuais confidenciais
   - **Criptografia de disco do SO confidencial**: Habilitado.
   - **Gerenciamento de chaves**: Criptografia de disco confidencial com uma chave gerenciada pela plataforma Para obter mais informações sobre como criar VMs confidenciais, consulte este artigo da Microsoft.
2. Prepare a imagem mestre na VM criada. Instale os aplicativos necessários e o VDA na VM criada.

> **Nota:**
>
> A criação de VMs confidenciais usando VHD não é suportada. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil da máquina usando uma destas formas:

   - Use a VM existente criada na etapa 1 se ela possuir as propriedades de máquina necessárias.
   - Se você optar por uma especificação de modelo ARM como perfil da máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos de VM confidencial, como *SecurityEncryptionType* e *diskEncryptionSet* (para chave gerenciada pelo cliente). Para obter mais informações, consulte Criar uma especificação de modelo do Azure.

     > **Nota:**
     >
     > - Certifique-se de que a imagem mestre e o perfil da máquina tenham o mesmo tipo de chave de segurança.
     > - Para criar VMs confidenciais que exigem criptografia de disco do SO confidencial com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil da máquina sejam idênticos.

**Criar VMs confidenciais usando o Web Studio ou comandos PowerShell**

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Web Studio, siga as etapas descritas em Criar catálogos de máquinas. Tenha as seguintes considerações em mente:

- Na página **Imagem**, selecione uma imagem mestre e um perfil de máquina que você preparou para a criação da VM confidencial. A seleção do perfil da máquina é obrigatória e apenas perfis que correspondem ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.

- Na página **Máquinas Virtuais**, apenas os tamanhos de máquina que suportam VMs confidenciais aparecem para seleção.
- Na página **Configurações de Disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

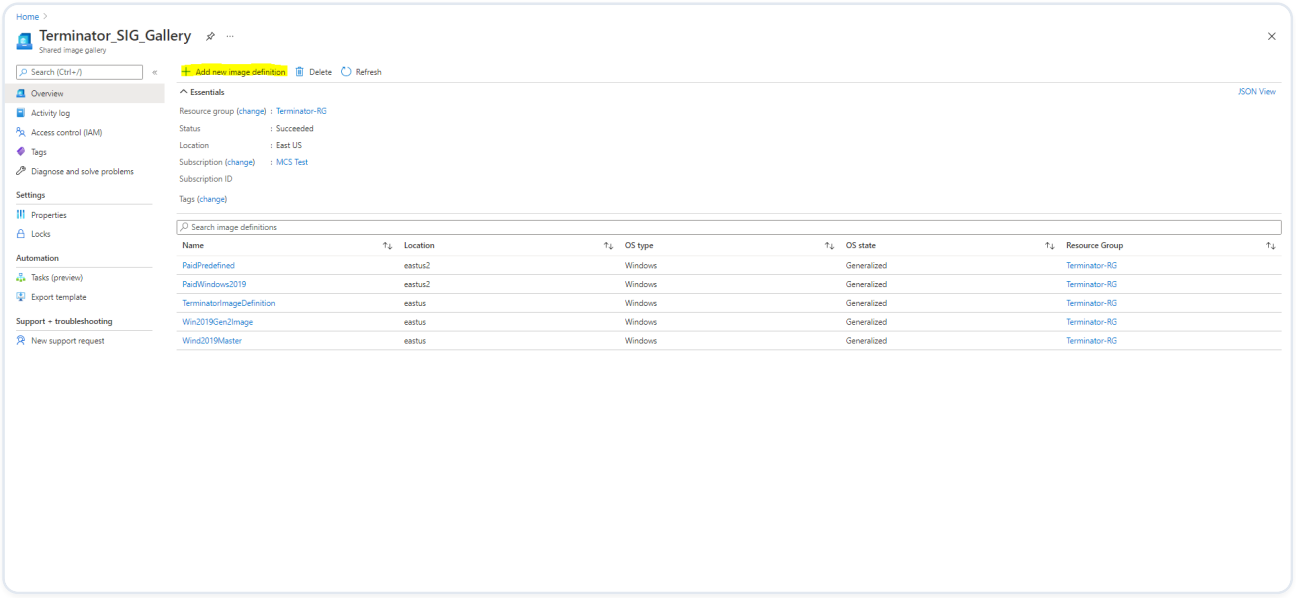
### Azure Marketplace

O Citrix Virtual Apps and Desktops oferece suporte ao uso de uma imagem mestre no Azure que contém informações de plano para criar um catálogo de máquinas. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**
>
> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não anexam informações de plano. O recurso do Citrix Virtual Apps and Desktops é para imagens pagas.

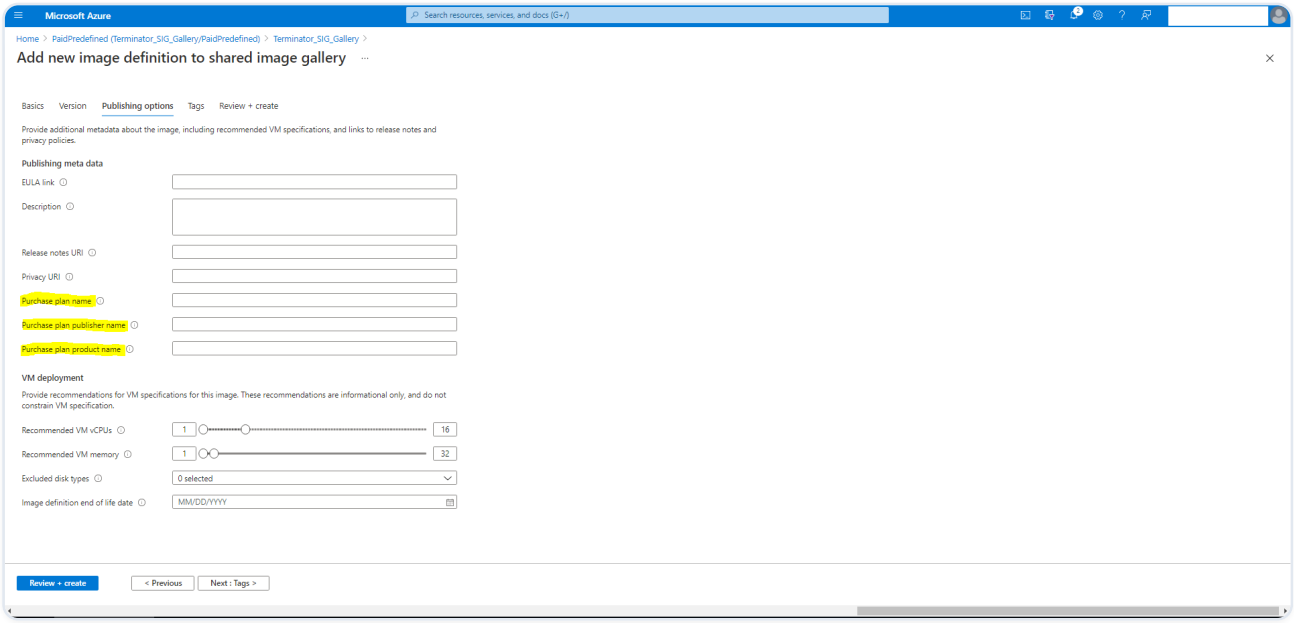
#### Certifique-se de que a imagem criada na Galeria de Imagens Compartilhadas contenha informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Essas imagens podem ser usadas opcionalmente para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.

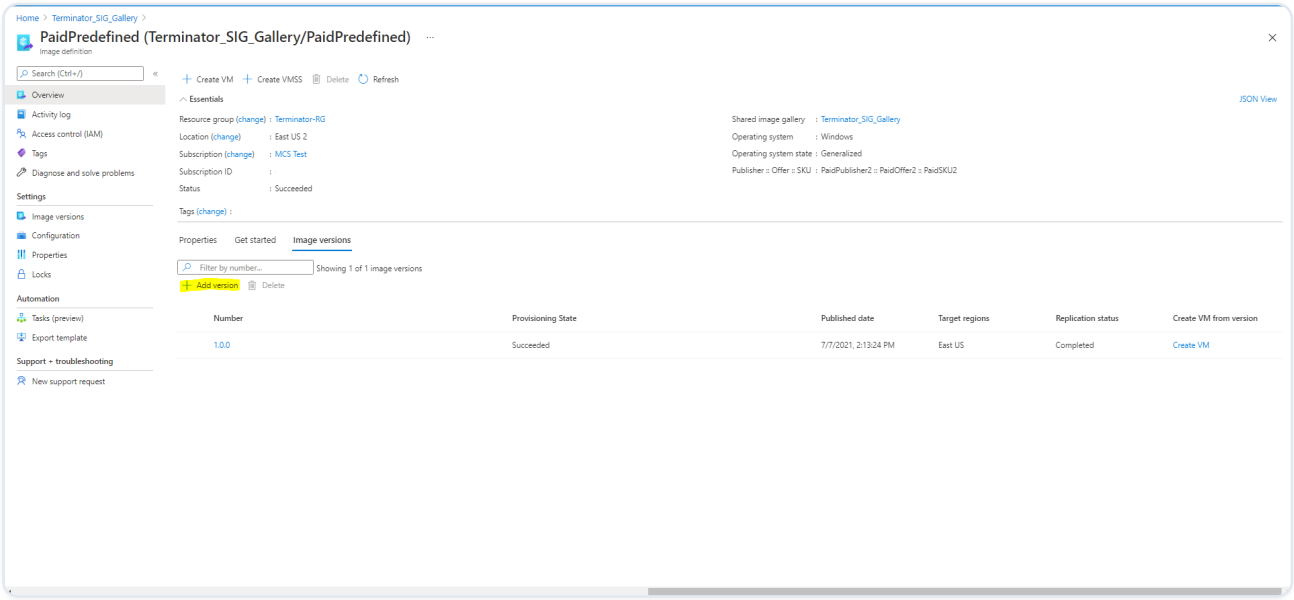



Na página **Opções de publicação**, verifique as informações do plano de compra.

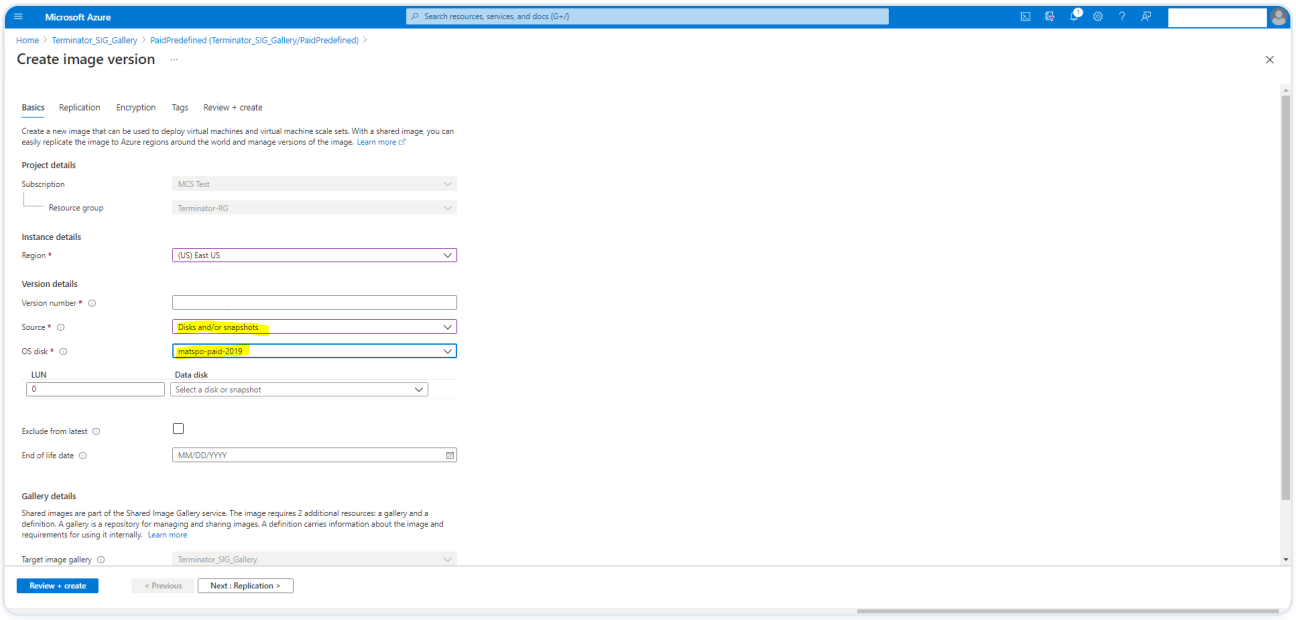
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. A falha ao preencher as informações do plano de compra pode fazer com que o processo de catálogo de máquinas falhe.




Após verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Esta é usada como a imagem mestre. Clique em **Adicionar versão**:




Na seção **Detalhes da versão**, selecione o instantâneo da imagem ou o disco gerenciado como a origem:




## Criar um catálogo de máquinas usando PowerShell

Esta seção detalha como você pode criar catálogos usando PowerShell:

- Criar um catálogo com disco de cache de gravação não persistente
- Criar um catálogo com disco de cache de write-back persistente
- Melhorar o desempenho de inicialização com MCSIO
- Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell
- Catálogos de máquinas com inicialização confiável
- Usar valores de propriedade de perfil de máquina
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente(#create-a-machine-catalog-with-customer-managed-encryption-key)
- Criar um catálogo de máquinas com criptografia dupla
- Criar um catálogo com discos efêmeros do Azure
- Hosts dedicados do Azure
- Criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure
- Configurar a Galeria de Imagens Compartilhadas
- Provisionar máquinas em Zonas de Disponibilidade especificadas
- Tipos de armazenamento
- Local do arquivo de paginação
- Atualizar configuração do arquivo de paginação

- Criar um catálogo usando VMs Spot do Azure(#create-a-catalog-using-azure-spot-vms)
- Configurar tamanhos de VM de backup
- Copiar tags em todos os recursos
- Provisionar VMs de catálogo com o Agente do Azure Monitor instalado

### Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back não persistente, use o parâmetro 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 true ao executar `New-ProvScheme` se você quiser usar o disco temporário como disco de cache de write-back. Se esta propriedade não for especificada, o parâmetro é definido como **False** por padrão.

Por exemplo, usando o parâmetro `CustomProperties` para definir `UseTempDiskForWBC` como **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

**Nota:**

Depois de confirmar o catálogo de máquinas para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar VHD posteriormente.

### Criar um catálogo com disco de cache de write-back persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes de suportar `PersistWBC` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

Ao usar essas propriedades, considere que elas contêm valores padrão se as propriedades forem omitidas do parâmetro `CustomProperties`. A propriedade `PersistWBC` tem dois valores possíveis: **true** ou **false**.

Definir a propriedade `PersistWBC` como **true** não exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Web Studio.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Web Studio.

**Nota:**

Se a propriedade `PersistWBC` for omitida, a propriedade assume o valor padrão **false** e o cache de write-back é excluído quando a máquina é desligada usando o Web Studio.

Por exemplo, usando o parâmetro `CustomProperties` para definir `PersistWBC` como true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

**Importante:**

A propriedade `PersistWBC` só pode ser definida usando o cmdlet PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como true:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

### Melhorar o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada do PowerShell

`PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

Para habilitar este recurso, defina a propriedade personalizada `PersistOSDisk` como `true`. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
```
```

```
-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

### Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou comandos PowerShell.

Para o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio

Usando comandos PowerShell:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie ou atualize um catálogo.
    - Para criar um catálogo:
        a. Use o comando `New-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
```

```
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

b. Conclua a criação do catálogo.

- Para atualizar um catálogo, use o comando `Set-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

### Catálogos de máquinas com inicialização confiável

Para criar com êxito um catálogo de máquinas com inicialização confiável, use:

- Um perfil de máquina com inicialização confiável
- Um tamanho de VM que suporta inicialização confiável

- Uma versão de VM do Windows que suporta inicialização confiável. Atualmente, Windows 10, Windows 11, Windows Server 2016, 2019 e 2022 suportam inicialização confiável.

**Importante:**

O MCS suporta a criação de um novo catálogo com VMs habilitadas para inicialização confiável. No entanto, para atualizar um catálogo persistente existente e VMs existentes, você deve usar o portal do Azure. Você não pode atualizar a inicialização confiável de um catálogo não persistente. Para obter mais informações, consulte o documento da Microsoft Habilitar inicialização confiável em VMs do Azure existentes.

Para visualizar os itens de inventário da oferta do Citrix Virtual Apps and Desktops e determinar se o tamanho da VM oferece suporte à inicialização confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
   - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM oferece suporte à inicialização confiável.
   - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não oferece suporte à inicialização confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que oferecem suporte à inicialização confiável:

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

A seguir estão exemplos que descrevem se o tamanho da VM suporta inicialização confiável após você executar o comando do Azure PowerShell.

- *Exemplo 1*: Se a VM do Azure suportar apenas a Geração 1, essa VM não suporta inicialização confiável. Portanto, a capacidade `TrustedLaunchDisabled` não é exibida após você executar o comando do Azure PowerShell.
- *Exemplo 2*: Se a VM do Azure suportar apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` for **True**, o tamanho da VM da Geração 2 não é suportado para inicialização confiável.
- *Exemplo 3*: Se a VM do Azure suportar apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` não for exibida após você executar o comando do PowerShell, o tamanho da VM da Geração 2 será suportado para inicialização confiável.

Para obter mais informações sobre a inicialização confiável para máquinas virtuais do Azure, consulte o documento da Microsoft Inicialização confiável para máquinas virtuais do Azure.

**Criar um catálogo de máquinas com inicialização confiável**

1. Crie uma imagem mestre habilitada com inicialização confiável. Consulte a documentação da Microsoft Imagens de VM de inicialização confiável.
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de inicialização confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft Deploy a trusted launch VM.
3. Crie um catálogo de máquinas usando o Web Studio ou comandos do PowerShell.
   - Se você quiser usar o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio.
   - Se você quiser usar comandos do PowerShell, use o comando `New-ProvScheme` com a VM ou a especificação de modelo como entrada de perfil de máquina. Para a lista completa de comandos para criar um catálogo, consulte Criando um catálogo.

     Exemplo de `New-ProvScheme` com VM como entrada de perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     ```

```
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
hine profile vm.vm>"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

Exemplo de `New-ProvScheme` com especificação de modelo como entrada de perfil de máquina:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

### Erros ao criar catálogos de máquinas com Inicialização Confiável

Você recebe erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com inicialização confiável:

| CENÁRIO | ERRO |
| --- | --- |
| Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado | `MachineProfileNotSupportedForUnmanagedCatalog` |
| Se você selecionar um perfil de máquina que suporte Inicialização Confiável ao criar um catálogo com disco não gerenciado como imagem mestre | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Se você não selecionar um perfil de máquina ao criar um catálogo gerenciado com uma fonte de imagem mestre com Inicialização Confiável como tipo de segurança | `MachineProfileNotFoundForTrustedLaunchMasterImage` |
| Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre | `SecurityTypeConflictBetweenMasterImageAndMachineProfile` |
| Se você selecionar um tamanho de VM que não suporte Inicialização Confiável, mas usar uma imagem mestre que suporte Inicialização Confiável ao criar um catálogo | `MachineSizeNotSupportTrustedLaunch` |

### Usar valores de propriedade do perfil da máquina

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

- Zona de disponibilidade
- ID do Grupo de Host Dedicado
- ID do Conjunto de Criptografia de Disco
- Tipo de SO
- Tipo de licença
- Tipo de armazenamento

Se essas propriedades personalizadas não forem definidas explicitamente, os valores das propriedades serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como perfil da máquina. Além disso, se `ServiceOffering` não for especificado, ele será definido a partir do perfil da máquina.

**Nota:**

Se algumas das propriedades estiverem ausentes do perfil da máquina e não forem definidas nas propriedades personalizadas, os valores padrão das propriedades serão aplicados onde for cabível.

A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` têm todas as propriedades definidas ou os valores são derivados do MachineProfile.

- Cenários do New-ProvScheme
  - MachineProfile tem todas as propriedades e CustomProperties não estão definidas. Exemplo:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem apenas LicenseType e OsType.

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">

  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
  value>"/>

  </CustomProperties>
  ```

- Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  As propriedades personalizadas têm prioridade. Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
  ```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Exemplo:
  - CustomProperties definem LicenseType e StorageAccountType
  - MachineProfile define LicenseType, OsType e Zones

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não é definido. Exemplo:
  - CustomProperties definem StorageType
  - MachineProfile especifica LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>
```

```
<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- Se o OsType não estiver nem em CustomProperties nem em MachineProfile, então:
  - O valor é lido da imagem mestre.
  - Se a imagem mestre for um disco não gerenciado, o OsType será definido como Windows. Exemplo:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

O valor da imagem mestre é gravado nas propriedades personalizadas, neste caso Linux.

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Cenários de Set-ProvScheme
  - Um catálogo existente com:
    - CustomProperties para `StorageAccountType` e OsType
    - Perfil da Máquina `mpA.vm` que define zonas
  - Atualizações:
    - Perfil da Máquina mpB.vm que define StorageAccountType
    - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define LicenseType e OsType

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- Um catálogo existente com:
  - CustomProperties para S`torageAccountType` e OsType
  - Perfil da Máquina `mpA.vm` que define StorageAccountType e LicenseType
- Atualizações:
  - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define StorageAccountType e OsType.

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- Um catálogo existente com:
  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define Zonas
- Atualizações:
  - Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  - `ServiceOffering` não é especificado

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
```

```
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

### Provisionar VMs de catálogo com o Agente do Azure Monitor instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e agir sobre dados de telemetria de seus ambientes Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos de computação, como máquinas virtuais, e entrega os dados ao Azure Monitor. Atualmente, ele suporta a coleta de Logs de Eventos, Syslog e métricas de Desempenho e os envia para as fontes de dados do Azure Monitor Metrics e Azure Monitor Logs.

Para habilitar o monitoramento, identificando exclusivamente as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

#### Requisitos

- Permissões: Certifique-se de ter as permissões mínimas do Azure, conforme especificado em Permissões do Azure necessárias e as seguintes permissões para usar o Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regra de Coleta de Dados: Configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar uma DCR, consulte Criar uma regra de coleta de dados. Uma DCR é específica da plataforma (Windows ou Linux). Certifique-se de criar uma DCR de acordo com a plataforma necessária. O AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e as fontes de dados, como Azure Monitor Metrics e Azure Monitor Logs.
- Espaço de Trabalho Padrão: Crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um, consulte Criar um espaço de trabalho do Log Analytics. Ao

coletar logs e dados, as informações são armazenadas em um espaço de trabalho. Cada um possui um ID de espaço de trabalho e um ID de recurso exclusivos. O nome do espaço de trabalho deve ser exclusivo para um determinado grupo de recursos. Após criar um, configure as fontes de dados e as soluções para armazenar seus dados nele.

- Extensão de monitoramento na lista de permissões: As extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões na lista de permissões definidas pela Citrix. Para visualizar a lista de extensões na lista de permissões, use o comando PoSH, `Get-ProvMetadataConfiguration`.
- Imagem Mestra: A Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso pode levar a arquivos residuais e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para provisionar VMs de catálogo com AMA habilitado:

1. Configurar um modelo de perfil de máquina.
    - Se você quiser usar uma VM como um modelo de perfil de máquina:
        a. Crie uma VM no portal do Azure.
        b. Ligue a VM.
        c. Adicione a VM à regra de coleta de dados em **Recursos**. Isso invoca a instalação do agente na VM do modelo.

> **Nota:**
>
> Se você precisar criar um catálogo Linux, configure uma máquina Linux.

    - Se você quiser usar a especificação de modelo como um modelo de perfil de máquina:
        a. Configure uma especificação de modelo.
        b. Adicione a seguinte extensão e associação de regra de coleta de dados à especificação de modelo gerada:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
```

```
"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
```

```
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. Crie ou atualize um catálogo de máquinas MCS existente.

   - Para criar um novo catálogo MCS:

     a. Selecione essa VM ou especificação de modelo como um perfil de máquina no Web Studio.

     b. Prossiga com as próximas etapas para criar o catálogo.

   - Para atualizar um catálogo MCS existente, use os seguintes comandos PoSH:

     - Para que as novas VMs obtenham o modelo de perfil de máquina atualizado, execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

     - Para atualizar VMs existentes com o modelo de perfil de máquina atualizado:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. Ligue as VMs do catálogo.
4. Vá para o portal do Azure e verifique se a extensão de monitoramento está instalada na VM e se a VM está aparecendo em Recursos do DCR. Após alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

#### Solução de problemas

Para obter informações sobre as diretrizes de solução de problemas para o Azure Monitor Agent, consulte o seguinte:

- https://learn.microsoft.com/pt-br/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/pt-br/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

As etapas detalhadas sobre como criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente são:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Digite `cd xdhyp:/`.
4. Digite `cd .\HostingUnits\(your hosting unit)`.
5. Digite `cd diskencryptionset.folder`.
6. Insira `dir` para obter a lista dos Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma string de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
```

```
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. Execute o comando New-ProvScheme: Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"
```

```
-CustomProperties $customProperties
```

11. Conclua a criação do catálogo de máquinas.

### Criar um catálogo de máquinas com criptografia dupla

Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e comandos do PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Use o portal do Azure para habilitar a criptografia dupla em repouso para discos gerenciados.
2. Para procurar DiskEncryptionSets disponíveis em sua conexão de hospedagem:
   a. Abra uma janela do **PowerShell**.
   b. Execute os seguintes comandos PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`:
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (ex. azure-east)
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Você pode usar um Id do `DiskEncryptionSet` para criar ou atualizar um catálogo usando propriedades personalizadas.
3. Se você quiser usar o fluxo de trabalho de perfil de máquina, crie uma VM ou especificação de modelo como entrada de perfil de máquina.
   - Se você quiser usar uma VM como entrada de perfil de máquina:
     a. Crie uma VM no Portal do Azure.
     b. navegar para **Discos>Gerenciamento de chaves** para criptografar a VM diretamente com qualquer `DiskEncryptionSetID`.
   - Se você quiser usar uma especificação de modelo como entrada de perfil de máquina:

a. No modelo, em `properties>storageProfile>osDisk>managedDisk`, adicione o parâmetro `diskEncryptionSet` e adicione o ID do DES de criptografia dupla.

4. Crie o catálogo de máquinas.

- Se estiver usando o Web Studio, faça uma das seguintes opções além das etapas em Criar catálogos de máquinas.

  ◦ Se você não usar o fluxo de trabalho baseado em perfil de máquina, na página **Configurações de Disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue criando o catálogo.

  ◦ Se estiver usando o fluxo de trabalho de perfil de máquina, na página **Imagem**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID de conjunto de criptografia de disco em suas propriedades.

  Todas as máquinas criadas no catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

- Se estiver usando comandos do PowerShell, faça um dos seguintes:

  ◦ Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada `DiskEncryptionSetId` no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'
```

```
-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. Conclua a criação de um catálogo usando o SDK remoto do PowerShell. Para obter informações sobre como criar um catálogo usando o SDK remoto do PowerShell, consulte

https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Todas as máquinas criadas no catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

### Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina) somente se o catálogo não foi 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:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

Após o sucesso, todas as novas VMs que você adicionar ao seu catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

### Verificar se o catálogo está criptografado duplamente

- No Web Studio:

  a. navegar para **Catálogos de Máquinas**.

b. Selecione o catálogo que você deseja verificar. Clique na guia **Propriedades do Modelo** localizada perto da parte inferior da tela.

c. Em **Detalhes do Azure**, verifique o ID do Conjunto de Criptografia de Disco em **Conjunto de Criptografia de Disco**. Se o ID DES do catálogo estiver em branco, o catálogo não está criptografado.

d. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.

- Usando o comando PowerShell:

a. Abra a janela do **PowerShell**.

b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

c. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

d. Recupere a propriedade personalizada ID do DES do catálogo de máquinas. Por exemplo:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.

### Criar um catálogo com discos efêmeros do Azure

Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **Nota:**
>
> Se a propriedade personalizada `UseEphemeralOsDisk` for definida como **false** ou um valor não for especificado, todos os VDAs provisionados continuarão a usar um disco de SO provisionado.

A seguir, um exemplo de conjunto de propriedades personalizadas a serem usadas no esquema de provisionamento:

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },

            {

                "Name": "SharedImageGalleryReplicaRatio",

                "Value": "40"

            },

            {

                "Name": "SharedImageGalleryReplicaMaximum",

                "Value": "10"
```

```
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

### Configurar um disco efêmero para um catálogo

Para configurar um disco de SO efêmero do Azure para um catálogo, use o parâmetro `UseEphemeralOsDisk` em `Set-ProvScheme`. Defina o valor do parâmetro `UseEphemeralOsDisk` como **true**.

**Nota:**

Para usar este recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
```

```
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

### Considerações importantes para discos efêmeros

Para provisionar discos de SO efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve suportar discos de SO efêmeros.
- O tamanho do cache ou do disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco do SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também estas questões ao:

- Criar o esquema de provisionamento.
- Modificar o esquema de provisionamento.
- Atualizar a imagem.

## Hosts dedicados do Azure

Você pode usar o MCS para provisionar VMs em hosts dedicados do Azure. Antes de provisionar VMs em hosts dedicados do Azure:

- Criar um grupo de hosts.
- Criar hosts nesse grupo de hosts.
- Certifique-se de que há capacidade de host suficiente reservada para a criação de catálogos e máquinas virtuais.

Você pode criar um catálogo de máquinas com locação de host definida através do seguinte script PowerShell:

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
```

```
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade do catálogo e não pode ser alterado depois que o catálogo é criado. A locação dedicada não é atualmente suportada no Azure.
- Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`.
- O posicionamento automático do Azure é necessário. Essa funcionalidade faz uma solicitação para integrar a assinatura associada ao grupo de hosts. Para obter mais informações, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Se o posicionamento automático não estiver habilitado, o MCS gerará um erro durante a criação do catálogo.

### Criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure

Ao selecionar uma imagem para usar na criação de um catálogo de máquinas, você pode selecionar imagens que criou na Galeria de Computação do Azure.

Para que essas imagens apareçam, você deve:

1. Configure um site do Citrix Virtual Apps and Desktops.
2. Conecte-se ao Azure Resource Manager.
3. No portal do Azure, crie um grupo de recursos. Para obter detalhes, consulte Criar uma Galeria de Computação do Azure usando o portal.
4. No grupo de recursos, crie uma Galeria de Computação do Azure.
5. Na Galeria de Computação do Azure, crie uma definição de imagem.
6. Na definição de imagem, crie uma versão de imagem.

Use os seguintes comandos do PowerShell para criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

3. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

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

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Configurar Galeria de Imagens Compartilhadas

Use o comando `New-ProvScheme` para criar um esquema de provisionamento com suporte à Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para habilitar ou desabilitar esse recurso para um esquema de provisionamento e para alterar a taxa de réplicas e os valores máximos de réplicas.

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para oferecer suporte ao recurso de Galeria de Imagens Compartilhadas:

`UseSharedImageGallery`

- Define se a Galeria de Imagens Compartilhadas deve ser usada para armazenar as imagens publicadas. Se definido como **True**, a imagem é armazenada como uma imagem da Galeria de Imagens Compartilhadas; caso contrário, a imagem é armazenada como um instantâneo.
- Os valores válidos são **True** e **False**.
- Se a propriedade não for definida, o valor padrão é **False**.

`SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas da versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não for definida, os valores padrão são usados. O valor padrão para discos de SO persistentes é 1000 e o valor padrão para discos de SO não persistentes é 40.

`SharedImageGalleryReplicaMaximum`

- Define o número máximo de réplicas para cada versão de imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não for definida, o valor padrão é 10.
- Atualmente, o Azure oferece suporte a até 10 réplicas para uma única versão 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 o MCS registra e, em seguida, deixa a contagem atual de réplicas inalterada.

> **Dica:**

> Ao usar a Galeria de Imagens Compartilhadas para armazenar uma imagem publicada para catálogos provisionados pelo MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na taxa de réplicas e no máximo de réplicas. A contagem de réplicas é calculada dividindo o número de máquinas no catálogo pela taxa de réplicas (arredondando para o valor inteiro mais próximo) e, em seguida, limitando o valor à contagem máxima de réplicas. Por exemplo, com uma taxa de

> réplicas de 20 e um máximo de 5, 0 a 20 máquinas têm uma réplica criada, 21 a 40 têm 2 réplicas, 41 a 60 têm 3 réplicas, 61 a 80 têm 4 réplicas, 81+ têm 5 réplicas.

**Caso de uso: Atualizando a taxa de réplicas e o máximo de réplicas da Galeria de Imagens Compartilhadas**

O catálogo de máquinas existente usa a Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para atualizar as propriedades personalizadas para todas as máquinas existentes no catálogo e quaisquer máquinas futuras:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

**Caso de Uso: Convertendo um catálogo de instantâneos em um catálogo da Galeria de Imagens Compartilhadas**

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
```

```
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

**Dica:**

Os parâmetros `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` não são obrigatórios. Após a conclusão do comando `Set-ProvScheme`, a imagem da Galeria de Imagens Compartilhadas ainda não foi criada. Uma vez que o catálogo é configurado para usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. Reiniciar as máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Imagens Compartilhadas e todas as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente em algumas horas.

**Caso de Uso: Convertendo um Catálogo de Galeria de Imagens Compartilhadas para um catálogo de snapshot**

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

**Dica:**

Ao contrário da atualização de um snapshot para um catálogo de Galeria de Imagens Compartilhadas, os dados personalizados para cada máquina ainda não são atualizados para refletir as novas propriedades personalizadas. Execute o seguinte comando para ver as propriedades personalizadas originais da Galeria de Imagens Compartilhadas: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Após a conclusão do comando `Set-ProvScheme`, o snapshot da imagem ainda não foi criado. Uma vez que o catálogo é configurado para não usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada como um snapshot. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o snapshot e todas as máquinas recém-provisionadas são criadas a partir do snapshot. Reiniciar as máquinas as atualiza, momento em que os dados personalizados da máquina são atualizados para refletir que `UseSharedImageGallery` está definido como **False**. Os ativos antigos da Galeria de Imagens Compartilhadas (galeria, imagem e versão) são automaticamente limpos em algumas horas.

### Provisionar máquinas em Zonas de Disponibilidade especificadas

Você pode provisionar máquinas em Zonas de Disponibilidade específicas em ambientes Azure. Você pode conseguir isso usando o PowerShell.

**Nota:**

Se nenhuma zona for especificada, o MCS permite que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribui aleatoriamente as máquinas entre elas.

#### Configurar Zonas de Disponibilidade via PowerShell

Usando o PowerShell, você pode visualizar os itens do inventário de ofertas usando `Get-Item`. Por exemplo, para visualizar a oferta de serviço `Standard_B1ls` da *região Leste dos EUA*:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

Para visualizar as zonas, use o parâmetro `AdditionalData` para o item:

`$serviceOffering.AdditionalData`

Se as Zonas de Disponibilidade não forem especificadas, não haverá alteração na forma como as máquinas são provisionadas.

Para configurar Zonas de Disponibilidade via PowerShell, use a propriedade personalizada **Zones** disponível com a operação `New-ProvScheme`. A propriedade **Zones** define uma lista de Zonas de Disponibilidade para provisionar máquinas. Essas zonas podem incluir uma ou mais Zonas de Disponibilidade. Por exemplo, `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` para as Zonas 1 e 3.

Use o comando `Set-ProvScheme` para atualizar as zonas de um esquema de provisionamento.

Se uma zona inválida for fornecida, o esquema de provisionamento não será atualizado e uma mensagem de erro aparecerá fornecendo instruções sobre como corrigir o comando inválido.

> **Dica:**

> Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro relevante aparecerá.

### Tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes Azure que usam MCS. Para VMs de destino, o MCS suporta:

- Disco do SO: SSD premium, SSD ou HDD
- Disco de cache de gravação: SSD premium, SSD ou HDD

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM suporta o tipo de armazenamento selecionado.
- Se sua configuração usa um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

> **Dica:**

> `StorageType` é configurado para um tipo de SO e conta de armazenamento. `WBCDiskStorageType` é configurado para o tipo de armazenamento de cache de write-

> back. Para um catálogo normal, `StorageType` é necessário. Se `WBCDiskStorageType` não estiver configurado, `StorageType` é usado como padrão para `WBCDiskStorageType`.

> Se WBCDiskStorageType não estiver configurado, então StorageType é usado como padrão para WBCDiskStorageType

### Configurar tipos de armazenamento

Para configurar os tipos de armazenamento para VM, use o parâmetro `StorageType` em `New-ProvScheme`. Defina o valor do parâmetro `StorageType` para um dos tipos de armazenamento suportados.

A seguir, um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

### Habilitar armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica seu disco gerenciado do Azure de forma síncrona em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser configurado usando propriedades personalizadas existentes ou através do modelo **MachineProfile**. O armazenamento ZRS também é suportado com o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow`

e `-DurationInMinutes -1`, e você pode alterar uma máquina existente de armazenamento LRS para ZRS.

**Limitações:**

- Suportado apenas para discos gerenciados
- Suportado apenas com unidades de estado sólido (SSD) premium e padrão
- Não compatível com `StorageTypeAtShutdown`
- Disponível apenas em certas regiões.
- O desempenho do Azure cai ao criar discos ZRS em escala. Portanto, para a primeira inicialização, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

### DEFINIR O ARMAZENAMENTO COM REDUNDÂNCIA DE ZONA COMO O TIPO DE ARMAZENAMENTO DE DISCO

Você pode selecionar o armazenamento com redundância de zona durante a criação inicial do catálogo ou pode atualizar seu tipo de armazenamento em um catálogo existente.

### SELECIONAR ARMAZENAMENTO COM REDUNDÂNCIA DE ZONA USANDO COMANDOS DO POWERSHELL

Ao criar um novo catálogo no Azure usando o comando PowerShell `New-ProvScheme`, use `Standard_ZRS` como valor em `StorageAccountType`. Por exemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso de ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: A propriedade personalizada StorageTypeAtShutdown não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta exceção ocorre se você tentar usar o Armazenamento ZRS em uma Região do Azure que não suporta ZRS
- **ZrsRequiresManagedDisks**: Você pode usar o armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento de disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante a criação do catálogo, o disco do SO do perfil da máquina `StorageType` é usado se as propriedades personalizadas não estiverem definidas.

### Capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina ao criar um catálogo de máquinas, atualizar um catálogo de máquinas existente e atualizar VMs existentes.

Você pode criar uma VM ou especificação de modelo como uma fonte de perfil de máquina.

#### Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação do modelo.
    - Conta de armazenamento
    - Espaço de trabalho do Log Analytics
    - Namespace do hub de eventos com o preço da camada padrão
2. Criar fonte de perfil de máquina.
3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize VMs existentes.

#### Configurar IDs necessárias no Azure

Configure um dos seguintes no Azure:

- Conta de armazenamento
- Espaço de trabalho do Log Analytics
- Namespace do hub de eventos com o preço da camada Standard

### CONFIGURAR UMA CONTA DE ARMAZENAMENTO

Crie uma conta de armazenamento padrão no Azure. Na especificação do modelo, forneça o resourceId completo para a conta de armazenamento como o `storageAccountId`.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, os dados podem ser encontrados no contêiner `insights-metrics-pt1m`.

### CONFIGURAR UM ESPAÇO DE TRABALHO DO LOG ANALYTICS

Crie um espaço de trabalho do Log Analytics. Na especificação do modelo, forneça o resourceId completo para o espaço de trabalho do Log Analytics como o workspaceId.

Depois que as VMs são configuradas para registrar dados no espaço de trabalho, os dados podem ser consultados em Logs no Azure. Você pode executar o seguinte comando no Azure em Logs para mostrar uma contagem de todas as métricas registradas por um recurso:

```
AzureMetrics | summarize Count=count() by ResourceId
```

### CONFIGURAR UM HUB DE EVENTOS

Faça o seguinte para configurar um hub de eventos no portal do Azure:

1. Crie um namespace do hub de eventos com o preço da camada padrão.
2. Crie um hub de eventos sob o namespace.
3. navegar para **Captura** sob o hub de eventos. Ative o botão para capturar com o tipo de saída Avro.
4. Crie um novo contêiner em uma conta de armazenamento existente para capturar os logs.
5. Na especificação do modelo, especifique o `eventHubAuthorizationRuleId` no seguinte formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique o nome do hub de eventos.

Depois que as VMs são configuradas para registrar dados no hub de eventos, os dados são capturados no contêiner de armazenamento configurado.

#### Criar uma origem de perfil de máquina

Você pode criar uma VM ou especificação de modelo como uma origem de perfil de máquina.

### CRIAR UM PERFIL DE MÁQUINA BASEADO EM VM COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você quiser criar uma VM como seu perfil de máquina, então primeiro configure as configurações de diagnóstico na própria VM do modelo. Você pode consultar as instruções detalhadas fornecidas na documentação da Microsoft Configurações de diagnóstico no Azure Monitor.

Você pode executar os seguintes comandos para verificar se agora há configurações de diagnóstico associadas à VM ou NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

### CRIAR UM PERFIL DE MÁQUINA BASEADO EM ESPECIFICAÇÃO DE MODELO COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você deseja usar uma VM que já tem as configurações de diagnóstico habilitadas e exportá-la para uma especificação de modelo ARM, essas configurações não serão incluídas automaticamente no modelo. Você deve adicionar ou modificar manualmente as configurações de diagnóstico dentro do modelo ARM.

No entanto, se você deseja uma VM como seu perfil de máquina, o MCS garante que as configurações de diagnóstico críticas sejam capturadas com precisão e aplicadas aos recursos dentro do seu catálogo MCS.

1. Crie uma especificação de modelo padrão que defina uma VM e NIC(s).
2. Adicione recursos adicionais para implantar as configurações de diagnóstico de acordo com a especificação: Microsoft.Insights diagnosticSettings. Para o escopo, faça referência a uma VM ou NIC que esteja no modelo pelo nome com um ID parcial. Por exemplo, para criar configurações de diagnóstico anexadas a uma VM chamada test-VM na especificação do modelo, especifique o escopo como:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use a especificação do modelo como uma origem de perfil de máquina.

### Criar ou atualizar um catálogo com configurações de diagnóstico

Depois de criar uma origem de perfil de máquina, agora você pode criar um catálogo de máquinas usando o comando `New-ProvScheme`, atualizar um catálogo de máquinas existente usando o comando `Set-ProvScheme` e atualizar VMs existentes usando o comando `Request-ProvVMUpdate`.

## Local do arquivo de paginação

Em ambientes Azure, o arquivo de paginação é configurado em um local apropriado quando a VM é criada pela primeira vez. A configuração do arquivo de paginação é configurada no formato `<page file location>[min size] [max size]` (o tamanho está em MB). Para obter mais informações, consulte o documento da Microsoft Como determinar o arquivo de paginação apropriado.

Ao criar `ProvScheme` durante a preparação da imagem, o MCS determina o local do arquivo de paginação com base em certas regras. Depois de criar `ProvScheme`:

- A alteração do tamanho da VM é 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 é bloqueada se a oferta de serviço for alterada devido à atualização do perfil da máquina, fazendo com que a configuração do arquivo de paginação seja diferente.
- As propriedades do disco de SO efêmero (EOS) e MCSIO não podem ser alteradas.

### Determinação do local do arquivo de paginação

Recursos como EOS e MCSIO têm seu próprio local de arquivo de paginação esperado e são exclusivos um do outro. A tabela mostra o local de arquivo de paginação esperado para cada recurso:

| RECURSO | LOCAL ESPERADO DO ARQUIVO DE PAGINAÇÃO |
|---|---|
| EOS | Disco do SO |
| MCSIO | Primeiro, disco temporário do Azure; caso contrário, disco de cache de write-back |

> **Nota:**

> Mesmo que a preparação da imagem seja desacoplada da criação do esquema de provisionamento, o MCS determina corretamente o local do arquivo de paginação. O local padrão do arquivo de paginação é no 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 da 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 da 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 da imagem de origem é definido no disco temporário, enquanto o disco de SO efêmero está habilitado no esquema de provisionamento. | O arquivo de paginação é colocado no disco do SO |
| Atualização do esquema de provisionamento | Você tenta atualizar o esquema de provisionamento, o tamanho da VM original tem disco temporário e a VM de destino não tem disco temporário. | Rejeita a alteração com uma mensagem de erro |

| DURANTE | CENÁRIO | RESULTADO |
| --- | --- | --- |
| Atualização do esquema de provisionamento | Você tenta atualizar o esquema de provisionamento, o tamanho da VM original 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 paginação

Você também pode especificar a configuração do arquivo de paginação, incluindo o local e o tamanho, explicitamente usando o comando PowerShell. Isso substitui o valor determinado pelo MCS. Você pode fazer isso executando o comando `New-ProvScheme` e incluindo as seguintes propriedades personalizadas:

- `PageFileDiskDriveLetterOverride`: Letra da unidade de disco do local do arquivo de paginação
- `InitialPageFileSizeInMB`: Tamanho inicial do arquivo de paginação em MB
- `MaxPageFileSizeInMB`: Tamanho máximo do arquivo de paginação em MB

Exemplo de uso das propriedades personalizadas:

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property
xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride" Value="d"/>
`


<Property
xsi:type="StringProperty" Name="InitialPageFileSizeInMB" Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value="8196"/
> `

<Property
```

```
xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `

<Property
xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `

</CustomProperties>'
```

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 paginação não pode ser alterada posteriormente.
- Forneça todas as propriedades relativas à configuração do arquivo de paginação (`PageFileDiskDriveLetterOverride`, `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.
- Este recurso não é compatível com o Web Studio.

### Criar um catálogo usando VMs Spot do Azure

As VMs Spot do Azure permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa de custos. No entanto, a capacidade de alocar uma VM Spot do Azure depende da capacidade e dos preços atuais. Portanto, o Azure pode despejar sua VM em execução, falhar ao criar a VM ou falhar ao ligar a VM de acordo com a Política de despejo. Assim, as VMs Spot do Azure são boas para algumas aplicações e desktops não críticos. Para obter mais informações, consulte Usar Máquinas Virtuais Spot do Azure.

#### Limitações

- Nem todos os tamanhos de VM são suportados para VMs Spot do Azure. Para obter mais informações, consulte Limitações.

  Você pode executar o seguinte comando PowerShell para verificar se um tamanho de VM suporta VMs Spot ou não. Se um tamanho de VM suportar VM Spot, então `SupportsSpotVM` é **True**.

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
AdditionalData
```

- Atualmente, as VMs Spot do Azure não suportam hibernação.

**Requisito**

Ao criar a origem do perfil da máquina (VM ou especificação de modelo) para o catálogo de VMs Spot do Azure, você deve selecionar Instância Spot do Azure (se estiver usando VM) ou definir `priority` como `Spot` (se estiver usando especificação de modelo).

**Etapas para criar um catálogo usando VMs Spot do Azure**

1. Crie uma origem de perfil de máquina (VM ou modelo de inicialização).
   - Para criar uma VM usando o portal do Azure, consulte Implantar Máquinas Virtuais Spot do Azure usando o portal do Azure.
   - Para criar uma especificação de modelo, adicione as seguintes propriedades em **resources > type: Microsoft.Compute/virtualMachines > properties** na especificação de modelo. Por exemplo:

```
"priority": "Spot",

"evictionPolicy": "Deallocate",

"billingProfile": {

"maxPrice": 0.01

}
```

**Nota:**

- A política de remoção pode ser **Deallocate** ou **Delete**.
  - Para VMs não persistentes, o MCS sempre define a política de remoção como **Delete**. Se a VM for removida, ela será excluída junto com quaisquer discos não

persistentes (por exemplo, disco do SO). Quaisquer discos persistentes (por exemplo, disco de identidade) não são excluídos. No entanto, um disco do SO é persistente se o tipo de catálogo for persistente ou se a propriedade personalizada `PersistOsDisk` for definida como True. Da mesma forma, um disco WBC é persistente se a propriedade personalizada `PersistWbc` for definida como **True**.

- Para VMs persistentes, o MCS sempre define a política de remoção como Deallocate. Se a VM for removida, ela será desalocada. Nenhuma alteração é feita nos discos.

- O preço máximo é o preço que você está disposto a pagar por hora. Se você estiver usando **Somente Capacidade**, então este é **-1**. O preço máximo pode ser apenas nulo, -1 ou um decimal maior que zero. Para obter mais informações, consulte Preços.

2. Você pode executar o seguinte comando PowerShell para verificar se um perfil de máquina está habilitado para Azure Spot VM ou não. Se o parâmetro `SpotEnabled` for **True** e `SpotEvictionPolicy` estiver definido como **Deallocate** ou **Delete**, então o perfil de máquina estará habilitado para Azure Spot VM. Por exemplo,

   - Se a origem do perfil da máquina for uma VM, execute o seguinte comando:

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - Se a origem do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. Crie um catálogo de máquinas usando um perfil de máquina com o comando PowerShell `New-ProvScheme`.

Você pode atualizar um catálogo usando o comando `Set-ProvScheme`. Você também pode atualizar VMs existentes usando o comando PowerShell `Set-ProvVmUpdateTimeWindow`. O perfil da máquina é atualizado no próximo ligar.

#### Remoções em uma VM Spot do Azure em execução

Se a capacidade de computação estiver indisponível ou o preço por hora for superior ao preço máximo configurado, o Azure removerá uma VM Spot em execução. Por padrão, você não é notificado de uma remoção. A VM simplesmente congela e é removida. A Microsoft recomenda usar Eventos Agendados para monitorar remoções. Consulte Monitorar continuamente para remoção. Você também pode executar scripts de dentro de uma VM para receber uma notificação antes da remoção. Por exemplo, a Microsoft tem um script de sondagem em Python ScheduledEvents.cs.

#### Solução de problemas

- Você pode ver as propriedades da VM Spot em customMachineData da VM provisionada usando o comando `Get-ProvVM`. Se o campo de prioridade estiver definido como **Spot**, então o Spot está em uso.
- Você pode verificar se uma VM está usando Spot no Portal do Azure:

  a. Encontre a VM no Portal do Azure.

  b. Vá para a página **Visão geral**.

  c. Role para baixo até o final e localize a seção **Azure Spot**.

    - Se o Spot não estiver em uso, este campo estará vazio.
    - Se o Spot estiver em uso, os campos **Azure Spot** e **Política de remoção do Azure Spot** estarão definidos.

1. Você pode verificar o perfil de faturamento ou o preço máximo por hora para a VM na página de Configuração.

### Configurar tamanhos de VM de backup

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

`BackupVmConfiguration` ao criar ou atualizar um catálogo de máquinas MCS. O MCS tenta recorrer aos tamanhos de VM de backup na ordem fornecida por você na lista.

Quando o MCS usa uma configuração de backup específica para a VM, ele continua a usar essa configuração até o próximo desligamento. No próximo ligamento, o MCS tenta inicializar a configuração primária da VM. Em caso de falha, o MCS tenta novamente inicializar uma configuração de tamanho de VM de backup conforme a lista.

Este recurso é compatível com:

- um catálogo que usa um perfil de máquina
- catálogos de máquinas MCS persistentes e não persistentes
- ambientes Azure atualmente

### Considerações importantes

- Você pode fornecer mais de um tamanho de VM de backup na lista.
- A lista deve ser única.
- Você pode adicionar a propriedade de tipo de instância para cada uma das VMs na lista. O tipo é **Spot** ou **Regular**. Se o tipo não for especificado, o MCS considera a VM como **Regular**.
- Você pode alterar a lista de tamanhos de VM de backup de um catálogo existente usando os comandos PowerShell `Set-ProvScheme`.
- Você pode atualizar as VMs existentes criadas a partir do esquema de provisionamento associado ao catálogo usando o comando `Set-ProvVMUpdateTimeWindow`.
- Você pode configurar a lista de 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 a usar a lista de tamanhos de VM de backup definida para essa VM específica, mesmo que a lista no esquema de provisionamento seja atualizada posteriormente. Você pode usar `Set-ProvVM` com `-RevertToProvSchemeConfiguration` para fazer com que a VM use a lista de backup no esquema de provisionamento.

### Criar um catálogo com tamanhos de VM de backup

> **Nota:**

> Para resolver o problema de congelamento da interface do usuário do Studio, substitua todas as aspas simples por `"` ao executar os comandos do PowerShell.

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
4. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
5. Crie um esquema de provisionamento com o perfil da máquina. Consulte Como configurar a configuração de backup.
6. Atualize o BrokerCatalog com o Id exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

### Atualizar um catálogo existente

Você pode atualizar um esquema de provisionamento usando o comando `Set-ProvScheme`. Consulte Como configurar a configuração de backup.

### Atualizar VMs existentes

Você pode atualizar VMs existentes em um catálogo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`. O comando atualiza as VMs criadas a partir do esquema de provisionamento associado ao catálogo no próximo ligar dentro da janela de tempo fornecida. Por exemplo:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Observação:**

> `StartsNow` indica o horário de início agendado. `DurationInMinutes` é a janela de tempo do agendamento.

> Você pode configurar a lista de tamanho de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Por exemplo:

1. Execute o comando `Set-ProvVM` para configurar a lista de tamanho de VM de backup para uma VM MCS existente selecionada. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. Execute o comando `Set-ProvVMUpdateTimeWindow` para aplicar as atualizações. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

### Copiar tags em todos os recursos

Você pode copiar tags especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do SO, disco de identidade e disco de cache de write-back) de uma nova VM ou de uma VM existente em um catálogo de máquinas. A origem do perfil da máquina pode ser uma VM ou uma especificação de modelo ARM.

**Nota:**

Você deve adicionar a política nas tags (consulte Atribuir definições de política para conformidade de tags) ou adicionar as tags em uma origem de perfil de máquina para reter as tags nos recursos.

#### Pré-requisitos

Crie a origem do perfil da máquina (VM ou especificação de modelo ARM) para ter tags na VM, discos e NICs dessa VM.

- Se você deseja ter uma VM como entrada de perfil de máquina, aplique tags na VM e em todos os recursos no portal do Azure. Consulte Aplicar tags com o portal do Azure.
- Se você deseja ter uma especificação de modelo ARM como entrada de perfil de máquina, adicione o seguinte bloco de tags em cada recurso.

```
 "tags": {

"TagC": "Value3"

},
```

**Nota:**

Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

### Copiar tags para os recursos de uma VM em um novo catálogo de máquinas

1. Crie um catálogo não persistente ou persistente com uma VM ou especificação de modelo ARM como entrada de perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

> **Nota:**
>
> Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs que você deseja que as VMs usem.

### Modificar tags nos recursos de uma VM existente

1. Crie um perfil de máquina com as tags em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. Desligue a VM na qual você deseja aplicar as atualizações.
4. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. Ligue a VM.
6. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes.

> **Nota:**
>
> Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs fornecidas no `Set-ProvScheme`.

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft Azure

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure Resource Manager
- Criar catálogos de máquinas

## Criar um catálogo do Microsoft System Center Virtual Machine Manager

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

> **Observação:**
>
> Antes de criar um catálogo VMM, você precisa concluir a criação de uma conexão com o VMM. Consulte Conexão com o Microsoft System Center Virtual Machine Manager.

### Criar uma VM mestre

1. Instale um VDA na VM mestre e selecione a opção para otimizar a área de trabalho para melhorar o desempenho.
2. Tire um instantâneo da VM mestre para usar como backup.
3. Crie áreas de trabalho virtuais.

### MCS em compartilhamentos de arquivos SMB 3

Para catálogos de máquinas criados com MCS em compartilhamentos de arquivos SMB 3 para armazenamento de VM, certifique-se de que as credenciais atendam aos seguintes requisitos. Esses requisitos garantem que as chamadas da Biblioteca de Comunicações do Hypervisor (HCL) do Controller se conectem com sucesso ao armazenamento SMB:

- As credenciais de usuário do VMM devem incluir acesso total de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante os eventos do ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Ao usar o armazenamento SMB, habilite o Provedor de Suporte de Segurança de Credencial de Autenticação (CredSSP) do Controller para máquinas Hyper-V individuais. Use este processo para VMM 2012 SP1 com Hyper-V no Windows Server 2012. Para obter mais informações, consulte CTX137465.

A HCL usa `CredSSP` para abrir uma conexão com a máquina Hyper-V. Esse recurso passa credenciais de usuário criptografadas por Kerberos para a máquina Hyper-V. Os comandos do **PowerShell** na sessão na máquina Hyper-V remota são executados com as credenciais fornecidas. Neste caso, as credenciais do usuário VMM, para que os comandos de comunicação para o armazenamento funcionem corretamente.

As seguintes tarefas usam scripts PowerShell que se originam na HCL e são então enviados para a máquina Hyper-V para atuar no armazenamento SMB 3.0.

- **Consolidar imagem mestre**: Uma imagem mestre cria um esquema de provisionamento MCS (catálogo de máquinas). Ela clona e nivela a VM mestre pronta para criar VMs a partir do novo disco criado (e remove a dependência da VM mestre original).

  ConvertVirtualHardDisk no namespace root\\virtualization\\v2

  Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **Criar disco de diferença:** Cria um disco de diferença a partir da imagem mestre gerada pela consolidação da imagem mestre. O disco de diferença é então anexado a uma nova VM.

  CreateVirtualHardDisk no namespace root\\virtualization\\v2

  Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **Carregar discos de identidade:** A HCL não pode carregar diretamente o disco de identidade para o armazenamento SMB. Portanto, a máquina Hyper-V deve carregar e copiar o disco de identidade para o armazenamento. Como a máquina Hyper-V não pode ler o disco do Controller, a HCL deve primeiro copiar o disco de identidade através da máquina Hyper-V da seguinte forma.

  a. O HCL carrega a Identidade para a máquina Hyper-V através do compartilhamento do administrador.

  b. A máquina Hyper-V copia o disco para o armazenamento SMB através de um script PowerShell executado na sessão remota do PowerShell. Uma pasta é criada na máquina Hyper-V e as permissões nessa pasta são bloqueadas apenas para o usuário VMM (através da conexão remota do PowerShell).

  c. O HCL exclui o arquivo do compartilhamento do administrador.

  d. Quando a HCL termina de carregar o disco de identidade para a máquina Hyper-V, a sessão remota do PowerShell copia os discos de identidade para o armazenamento SMB. Em seguida, ela os exclui da máquina Hyper-V.

  A pasta do disco de identidade é recriada se for excluída para que esteja disponível para reutilização.

- **Baixar discos de identidade:** Assim como nos uploads, os discos de identidade passam pela máquina Hyper-V para a HCL. O processo a seguir cria uma pasta que tem apenas permissões de usuário VMM no servidor Hyper-V, caso ela não exista.

  a. A máquina Hyper-V copia o disco do armazenamento SMB para o armazenamento local do Hyper-V através de um script PowerShell. Este script é executado na sessão remota do PowerShell V3.

  b. O HCL lê o disco do compartilhamento do administrador da máquina Hyper-V para a memória.

  c. O HCL exclui o arquivo do compartilhamento do administrador.

## Criar um catálogo com um perfil de máquina

Você pode usar um perfil de máquina para criar e atualizar um catálogo de máquinas MCS em ambientes do System Center Virtual Machine Manager (SCVMM). Você também pode habilitar a virtualização aninhada e o vTPM.

### Considerações importantes

- A imagem mestre só pode ser um instantâneo e não uma VM.
- Você só pode usar a VM como a origem do perfil de máquina.
- Você pode configurar o VTPM a partir do console do Hyper-V e não do console do SCVMM.
- Se a imagem mestre tiver o vTPM habilitado, você deverá habilitar o vTPM na origem do perfil de máquina.
- O vTPM é suportado apenas em máquinas de Geração 2.
- Os seguintes parâmetros sobrescrevem os valores capturados em um perfil de máquina se fornecidos separadamente:
  - VMCpuCount
  - VMMemoryMB
  - Armazenamento em disco
- Você pode atualizar um catálogo existente usando o comando `Set-ProvScheme`.

### Etapas para criar um catálogo usando um perfil de máquina

1. Crie uma VM para ser uma fonte de perfil de máquina. Para obter mais informações, consulte Provisionar máquinas virtuais no tecido VMM. Você não pode alterar a **Geração** depois de selecionada.
   - Se você quiser habilitar a virtualização aninhada, selecione a caixa de seleção **Habilitar Virtualização Aninhada** na página **Selecionar Origem**.
   - Se você quiser habilitar o vTPM, depois de criar a VM, faça login no host Hyper-V e encontre sua VM em **Gerenciador do Hyper-V**. Clique com o botão direito do mouse na VM e vá para **Configurações**. Em **Segurança**, selecione a caixa de seleção **Habilitar Módulo de Plataforma Confiável**.
2. Abra uma janela do **PowerShell**.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

4. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
5. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
6. Crie um esquema de provisionamento com o perfil da máquina. Por exemplo:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. Atualiza o catálogo do Broker com o ID exclusivo do esquema de provisionamento.
8. Crie e adicione VMs ao catálogo.

Você pode atualizar um catálogo existente usando o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas

# Criar um catálogo Nutanix

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização Nutanix.

> **Nota:**
>
> Antes de criar um catálogo Nutanix, você precisa concluir a criação de uma conexão com o Nutanix. Consulte Conexão com Nutanix.

## Criar um catálogo de máquinas usando um snapshot do Nutanix

O snapshot selecionado é o modelo usado para criar as VMs no catálogo. Antes de criar o catálogo, crie imagens e snapshots no Nutanix. Para obter mais informações, consulte a documentação do Nutanix.

No assistente de criação de catálogo:

- As páginas **Sistema Operacional** e **Gerenciamento de Máquinas** não contêm informações específicas do Nutanix.
- A página **Container** ou **Cluster and Container** é exclusiva do Nutanix.

  Se você implantar máquinas usando o Nutanix AHV XI como recursos, verá a página **Contêiner**. Selecione um contêiner onde os discos de identidade das VMs serão colocados.

  Se você implantar máquinas usando o Nutanix AHV Prism Central (PC) como recursos, verá a página **Cluster e Contêiner**. Selecione qual cluster usar para a implantação de VMs e, em seguida, um contêiner.
- Na página **Imagem**, selecione o snapshot da imagem. Os nomes de snapshot do Acropolis devem ser prefixados com "XD_" para serem usados no Citrix Virtual Apps and Desktops. Use o console do Acropolis para renomear seus snapshots, se necessário. Se você renomear snapshots, reinicie o assistente de criação de catálogo para ver uma lista atualizada.
- Na página **Virtual Machines**, indique o número de CPUs virtuais e o número de núcleos por vCPU.
- Na página **Placas de Rede**, selecione o tipo de NIC para filtrar as redes associadas. Existem dois tipos de NIC: **VLAN** e **OVERLAY**. Selecione uma ou mais NICs que a imagem mestre contém e, em seguida, selecione uma rede virtual associada para cada NIC.

- As páginas **Machine Identities**, **Domain Credentials**, **Scopes** e **Summary** não contêm informações específicas do Nutanix.

### Limitação

Ao criar um catálogo MCS com conexão de host Nutanix (especificamente, plug-in Nutanix AHV 2.7.1), o tamanho do disco rígido das VMs provisionadas é exibido incorretamente no Web Studio. O tamanho exibido é muito menor (1 GB) do que o tamanho real de armazenamento (50 GB). O tamanho do disco rígido é exibido corretamente no console do Nutanix.

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Nutanix
- Conexão com a nuvem Nutanix e soluções de parceiros
- Criar catálogos de máquinas

## Criar um catálogo VMware

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

> **Observação:**
>
> Antes de criar um catálogo VMware, você precisa concluir a criação de uma conexão com o VMware. Consulte Conexão com o VMware.

### Criar uma VM mestre

Use uma VM mestre para fornecer desktops e aplicativos de usuário em um catálogo de máquinas. No seu hipervisor:

1. Instale um VDA na VM mestre, selecionando a opção de otimizar o desktop, o que melhora o desempenho.

2. Tire um instantâneo da VM mestre para usar como backup.

**Observação:**

Você pode usar o MCS para provisionar VMs no ambiente vSAN 8.0.

### Criar um catálogo de máquinas usando um perfil de máquina

Você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A origem da entrada do perfil de máquina é um modelo VMware. O perfil de máquina captura as propriedades de hardware de um modelo VMware e as aplica às VMs recém-provisionadas no catálogo.

**Observação:**

- A entrada da imagem mestre (instantâneo) e a entrada do perfil da máquina (modelo VMware) devem estar ambas com vTPM ativado ou ambas com vTPM desativado. Esta regra se aplica a `New-ProvScheme` e `Set-ProvScheme`.
- Se a imagem mestre estiver com vTPM ativado, o modelo VMware só poderá vir da mesma origem de VM que a imagem mestre.
- A política de armazenamento criptografado suporta apenas clone completo.
- Os catálogos baseados em perfil de máquina utilizam o modelo VMware fornecido para coletar informações do controlador de armazenamento, contando com os discos virtuais anexados. O modelo deve incluir um disco virtual que é necessário para recuperar as informações do controlador de armazenamento usadas para configurar discos virtuais para as máquinas virtuais.

O modelo VMware no perfil da máquina deve existir durante o ciclo de vida do catálogo para permitir o provisionamento de VMs para o catálogo. Sem um modelo VMware, você não pode provisionar novas VMs. Quando um modelo VMware é excluído, você deve fornecer um novo modelo usando o comando `Set-ProvScheme`.

- O MCS captura propriedades de um modelo VMware. Você pode criar um novo modelo VMware referenciando as propriedades armazenadas do modelo VMware usando o comando Get-Provscheme.

- Alternativamente, se o catálogo de máquinas e as VMs provisionadas existirem, uma máquina provisionada pelo MCS também pode ser usada para criar um novo modelo VMware.

Com base em diferentes sistemas operacionais, você pode criar um catálogo de máquinas com diferentes configurações:

- Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Portanto, o modelo VMware, que é uma fonte de perfil de máquina, deve ter o vTPM anexado a ele.
- Se o Windows 10 estiver instalado na imagem mestre sem vTPM anexado, você pode criar um catálogo de máquinas com um modelo VMware sem vTPM como fonte para o perfil da máquina.

Existe outra configuração onde você pode criar um catálogo de máquinas usando o modo de disco de cópia completa com um modelo de perfil de máquina aplicado com política de armazenamento criptografado.

- A "política de armazenamento criptografado" deve ser definida no modelo de perfil da máquina. Não a defina na VM Mestra.
- A abordagem de Clone de Cópia Completa está disponível apenas para provisionamento de Sistemas Operacionais persistentes de sessão única.

Para criar um catálogo de máquinas usando comandos PowerShell com perfil de máquina como entrada:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute os seguintes comandos:

    - Para criar um catálogo de máquinas com um modelo VMware com vTPM anexado como fonte para entrada de perfil de máquina e imagem mestre com Windows 11 instalado:

    ```
    $identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

    -NamingScheme "<string>-###"

    -NamingSchemeType Numeric

    -Domain "<domain name"
    ```

```
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"
```

```
-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas com um modelo VMware sem vTPM como fonte para perfil de máquina e imagem mestre com Windows 10 instalado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192
```

```
-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas usando o modo de disco de cópia completa com um modelo de perfil de máquina aplicado com política de armazenamento criptografado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

Para atualizar um perfil de máquina, use o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

### Verificar várias NICs

Você recebe várias mensagens de erro durante as verificações pré-voo para várias NICs ao usar um perfil de máquina e o parâmetro `NetworkMapping` nos comandos `New-ProvScheme` e `Set-ProvScheme`.

A lista de verificação pré-voo para várias NICs é a seguinte:

- Apenas a contagem de NICs do modelo de perfil da máquina é usada e validada. A rede para a qual essas NICs apontam não é usada ou validada em relação às redes da unidade de hospedagem.
- Se a contagem de NICs no modelo de perfil da máquina for maior que o número de redes na unidade de hospedagem, você receberá uma mensagem de erro.
- Se a contagem de NICs no modelo de perfil da máquina for zero, você receberá uma mensagem de erro. Quando a contagem de NICs no modelo de perfil da máquina for um, então:
  - Se nenhum mapeamento de rede for especificado no comando `New-ProvScheme` ou `Set-ProvScheme`, e a rede da unidade de hospedagem for uma, então a rede da unidade de hospedagem será usada.
  - Se o mapeamento de rede for especificado, então o mapeamento de rede especificado será usado se for válido.
- Quando a contagem de NICs no modelo de perfil da máquina for maior que 1, ou a contagem de redes da unidade de hospedagem for maior que 1, então:
  - É necessário um mapeamento de rede válido no comando, e ele deve fornecer mapeamento para cada NIC (ou seja, a contagem de NetworkMapping deve ser a mesma que a contagem de NICs do perfil da máquina).
  - Várias NICs não podem ser mapeadas para a mesma rede na unidade de hospedagem.
  - A contagem de `NetworkMapping` e a contagem de NICs do perfil da máquina devem ser menores ou iguais à contagem de redes da unidade de hospedagem.

- `NetworkMapping` deve ser fornecido para cada ID de 0 a n-1, onde n é o número de adaptadores de rede no modelo de perfil da máquina.

### Solução de problemas

Se a criação do catálogo falhar, consulte CTX294978.

### Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo VMware

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Criar catálogos de máquinas

# Pools de identidade de diferentes tipos de junção de identidade de máquina

Usando o MCS, você pode provisionar máquinas como ingressadas no AD local, híbridas do Microsoft Entra ou não ingressadas no domínio.

Para obter informações sobre como configurar identidades de máquina no Web Studio, consulte Criar catálogos de máquinas.

Para obter informações específicas sobre como criar catálogos com identidades de máquina ingressadas, consulte o seguinte:

- Pool de identidade de identidade de máquina ingressada no Microsoft Entra híbrido
- Pool de identidade de identidade de máquina não ingressada no domínio

## Pool de identidades de identidade de máquina híbrida unida ao Microsoft Entra

Este artigo descreve como criar catálogos híbridos ingressados no Microsoft Entra.

Para obter informações sobre requisitos, limitações e considerações, consulte Microsoft Entra híbrido unido.

### Usar o Web Studio

As informações a seguir são um suplemento à orientação em Criar catálogos de máquinas. Para criar catálogos híbridos ingressados no Azure AD, siga a orientação geral desse artigo, observando os detalhes específicos dos catálogos híbridos ingressados no Azure AD.

No assistente de criação de catálogo:

- Na página **Identidades da Máquina**, selecione **Microsoft Entra híbrido ingressado**. As máquinas criadas são de propriedade de uma organização e são conectadas com uma conta do Active Directory Domain Services que pertence a essa organização. Elas existem na nuvem e no local.

> **Observação:**
>
> Se você selecionar **Microsoft Entra híbrido ingressado** como o tipo de identidade, cada máquina no catálogo deve ter uma conta de computador AD correspondente.

### Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações no Web Studio. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

A diferença entre catálogos unidos ao AD local e catálogos híbridos do Microsoft Entra reside na criação do pool de identidades e das contas de máquina.

Para criar um pool de identidades junto com as contas para catálogos híbridos ingressados no Microsoft Entra:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
```

```
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

**Observação:**

`$password` é a senha correspondente para uma conta de usuário AD com Permissões de Gravação.

Todos os outros comandos usados para criar catálogos unidos ao Microsoft Entra híbrido são os mesmos que para catálogos tradicionais unidos ao AD local.

### Visualizar o status do processo de ingresso híbrido do Microsoft Entra

No Web Studio, o status do processo de ingresso híbrido do Microsoft Entra é visível quando as máquinas híbridas ingressadas no Microsoft Entra em um grupo de entrega estão em estado ligado. Para visualizar o status, use Pesquisar para identificar essas máquinas e, em seguida, para cada uma, verifique **Identidade da Máquina** na guia **Detalhes** no painel inferior. As seguintes informações podem aparecer em **Identidade da Máquina**:

- Unido hibridamente ao Microsoft Entra
- Ainda não ingressado no Azure AD

**Observação:**

- Você pode experimentar um ingresso híbrido atrasado do Microsoft Entra quando a máquina é ligada inicialmente. Isso é causado pelo intervalo de sincronização de identidade da máquina padrão (30 minutos do Microsoft Entra Connect). A máquina está no estado híbrido ingressado no Microsoft Entra somente depois que as identidades da máquina são sincronizadas com o Microsoft Entra ID através do Microsoft Entra Connect.
- Se as máquinas não conseguirem entrar no estado de junção híbrida do Microsoft Entra, elas não serão registradas no Delivery Controller. O status de registro delas aparece como **Inicialização**.

> Além disso, usando o Web Studio, você pode descobrir por que as máquinas estão indisponíveis. Para fazer isso, clique em uma máquina no nó **Pesquisar**, verifique **Registro** na guia **Detalhes** no painel inferior e, em seguida, leia a dica de ferramenta para obter informações adicionais.

### Solução de problemas

Se as máquinas não conseguirem ser unidas hibridamente ao Microsoft Entra, faça o seguinte:

- Verifique se a conta da máquina foi sincronizada com o Microsoft Entra ID através do portal do Microsoft Entra ID. Se sincronizada, **Ainda não ingressado no Azure AD** aparece, indicando o status de registro pendente.

  Para sincronizar contas de máquina com o Microsoft Entra ID, certifique-se de que:

  - A conta da máquina está na UO configurada para ser sincronizada com o Microsoft Entra ID. Contas de máquina sem o atributo **userCertificate** não são sincronizadas com o Microsoft Entra ID, mesmo que estejam na UO configurada para ser sincronizada.
  - O atributo **userCertificate** é preenchido na conta da máquina. Use o Active Directory Explorer para visualizar o atributo.
  - O Microsoft Entra Connect deve ter sido sincronizado pelo menos uma vez após a criação da conta da máquina. Caso contrário, execute manualmente o comando `Start-ADSyncSyncCycle -PolicyType Delta` no console do PowerShell da máquina do Microsoft Entra Connect para acionar uma sincronização imediata.

- Verifique se o par de chaves do dispositivo gerenciado pelo Citrix para o ingresso híbrido do Microsoft Entra foi corretamente enviado para a máquina consultando o valor de **DeviceKeyPairRestored** em **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verifique se o valor é 1. Caso contrário, as possíveis razões são:

  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `HybridAzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
  - A máquina não foi provisionada usando o mesmo esquema de provisionamento do catálogo de máquinas.
  - A máquina não está ingressada no domínio local. O ingresso no domínio local é um pré-requisito do Microsoft Entra hybrid joined.

- Verifique as mensagens de diagnóstico executando o comando `dsregcmd /status /debug` na máquina provisionada pelo MCS.
  - Se o Microsoft Entra hybrid join for bem-sucedido, **AzureAdJoined** e **DomainJoined** serão **SIM** na saída da linha de comando.
  - Caso contrário, consulte a documentação da Microsoft para solucionar os problemas: `<https://docs.microsoft.com/pt-br/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`.
  - Se você receber a mensagem de erro **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, então execute o seguinte comando PowerShell para reparar o certificado do usuário:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    Para obter mais informações sobre o problema do certificado do usuário, consulte CTX566696.

## Criar catálogos não associados a domínio

Este artigo descreve como criar catálogos não associados a domínio usando o Citrix Virtual Apps and Desktops.

Para obter informações sobre requisitos, limitações e considerações, consulte Não associado a domínio.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recurso
   - navegar para a UI de administração do Citrix Cloud™ > menu hambúrguer superior esquerdo > **Locais de Recursos**.
   - Clique em **+ Local de Recurso**.
   - Insira um nome para o novo local de recurso e clique em **Salvar**.
2. Crie uma conexão de hospedagem. Consulte a seção Criar e gerenciar conexões para obter detalhes.

Usando o Citrix Virtual Apps and Desktops, você pode criar catálogos baseados em grupos de trabalho ou máquinas não associadas a domínio. A criação de máquinas não associadas a

domínio depende de como o pool de identidades da conta é criado. O pool de identidades da conta é o mecanismo usado pelo MCS para criar e rastrear nomes de máquinas durante o provisionamento do catálogo.

Atualmente, você pode criar catálogos não associados a domínio apenas usando os comandos do PowerShell.

### Usar PowerShell

Você pode criar um pool de identidades para catálogos não associados a domínio usando o SDK do PowerShell Remoto.

Use os parâmetros do PowerShell, **WorkgroupMachine** e **IdentityType**, para criar um pool de identidades para catálogos não associados a domínio. Os parâmetros eliminam a necessidade de especificar todos os parâmetros específicos do AD, incluindo as credenciais de administrador de domínio:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

Todos os outros comandos usados para criar catálogos não associados a domínio são os mesmos que para os catálogos tradicionais associados ao Active Directory local.

# Gerenciar catálogos de máquinas

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

## Introdução

Você pode adicionar ou remover máquinas de um catálogo de máquinas, renomear, alterar a descrição ou gerenciar as contas de computador do Active Directory de um catálogo.

A manutenção de catálogos também pode incluir a garantia de que cada máquina tenha as atualizações mais recentes do sistema operacional. Incluindo atualizações de antivírus, atualizações de sistema operacional ou alterações de configuração.

- Os catálogos que contêm máquinas aleatórias agrupadas criadas usando o Machine Creation Services™ (MCS) mantêm as máquinas atualizando a imagem mestre usada no catálogo e, em seguida, atualizando as máquinas. Esse método permite que você atualize eficientemente um grande número de máquinas de usuário.
- Para catálogos que contêm máquinas estáticas, permanentemente atribuídas, e para catálogos de máquinas de Acesso Remoto a PC, você gerencia as atualizações das máquinas dos usuários fora do Web Studio. Execute esta tarefa individualmente ou coletivamente usando ferramentas de distribuição de software de terceiros.

Para obter informações sobre como criar e gerenciar conexões com hipervisores de host, consulte Conexões e recursos.

> **Nota:**
>
> O MCS não oferece suporte ao Windows 10 IoT Core e ao Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

### Sobre instâncias persistentes

Ao atualizar um catálogo MCS criado usando instâncias persistentes ou dedicadas, todas as novas máquinas criadas para o catálogo usam a imagem atualizada. As instâncias pré-existentes continuam a usar a instância original. O processo de atualização de uma imagem é feito da mesma forma para qualquer outro tipo de catálogo. Considere o seguinte:

- Com catálogos de disco persistentes, as máquinas pré-existentes não são atualizadas para a nova imagem, mas quaisquer novas máquinas adicionadas ao catálogo usam a nova imagem.
- Para catálogos de disco não persistentes, a imagem da máquina é atualizada na próxima vez que a máquina for redefinida.
- Com catálogos de máquinas persistentes, a atualização da imagem também atualiza as instâncias do catálogo que a utilizam.
- Para catálogos que não são persistentes, se você quiser imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

## Gerenciar catálogos de máquinas

Você pode gerenciar um catálogo de máquinas de duas maneiras:

- Usando o Web Studio
- Usando o PowerShell

## Usar o Web Studio

Esta seção detalha como você pode gerenciar catálogos usando o Web Studio:

- 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
- Organizar 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 este catálogo.

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Catálogo de Máquinas | O nome e o tipo de alocação do catálogo. Os tipos de alocação incluem |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| | Aleatório: As máquinas no catálogo são alocadas a um usuário aleatoriamente. |
| | Permanente: As máquinas no catálogo são alocadas a um usuário permanentemente. |
| Tipo de Máquina | O tipo de sessão suportado das máquinas no catálogo. Os valores possíveis incluem |
| | Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: Descartar. |
| | Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: No disco local |
| | Tipo de SO: SO de sessão única (Acesso remoto a PC) |
| | Tipo de SO: SO de sessão única (Virtual); Dados do usuário: Descartar |
| | Tipo de SO: SO de sessão única (Virtual); Dados do usuário: No disco local |
| Contagem de Máquinas | A contagem de máquinas no catálogo e o método de provisionamento. Os métodos de provisionamento possíveis incluem: Serviços de criação de máquina (máquina MCS), Manual e Serviços de provisionamento Citrix™. |
| Contagem Alocada | O número de máquinas no catálogo atribuídas a um grupo de entrega. |
| Pasta | O local do catálogo na árvore de **Catálogos de Máquinas**. Ele exibe o nome da pasta em que o catálogo está (incluindo a barra invertida final), ou `-` se o catálogo estiver no nível raiz. |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Atualização do VDA | Estado da Atualização do VDA. Os valores possíveis incluem: Não configurado, Agendado, Disponível e Atualizado. |
| Status da Imagem | O status de atualização da imagem do catálogo. Aplicável apenas a catálogos de máquinas não persistentes. Os valores possíveis incluem: Totalmente atualizado, Parcialmente atualizado, Atualizações pendentes, Preparando |

## Adicionar máquinas a um catálogo

Antes de começar:

- Certifique-se de que o host de virtualização tenha processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- Certifique-se de ter contas de computador do Active Directory não utilizadas suficientes. Se você estiver usando contas existentes, o número de máquinas que pode adicionar é limitado pelo número de contas disponíveis.
- Se você usar o Web Studio para criar contas de computador do Active Directory para as máquinas adicionais, deverá ter a permissão de administrador de domínio apropriada.

Para adicionar máquinas a um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar máquinas** na barra de ações.
4. Selecione o número de máquinas virtuais a serem adicionadas.
5. Se houver contas do Active Directory existentes insuficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas. Especifique um esquema de nomenclatura de conta, usando sinais de hash para indicar onde 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 nomeadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

6. Se você usar contas do Active Directory existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo .csv contendo nomes de contas. Certifique-se de que há contas suficientes para todas as máquinas que você está adicionando. O Web Studio gerencia essas contas. Permita que o Web Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

As máquinas são criadas como um processo em segundo plano e podem levar muito tempo ao criar muitas máquinas. A criação 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 foram copiados ou não são mais necessários.
- Todos os usuários estão desconectados. Ativar o modo de manutenção impede que novas conexões sejam feitas a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Exibir Máquinas** na barra de ações.
4. Selecione uma ou mais máquinas e, em seguida, selecione **Excluir** na barra de ações.

Escolha se deseja excluir as máquinas que estão sendo removidas. Se você optar por excluir as máquinas, indique se as contas do Active Directory para essas máquinas são mantidas, desabilitadas ou excluídas.

## Editar um catálogo

1. Na página **Descrição**, altere a descrição do catálogo.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Editar Catálogo de Máquinas** na barra de ações.
4. Na página **Escopos**, altere os escopos.
5. Você pode ver outras páginas dependendo do tipo de catálogo.

Para catálogos criados usando uma imagem do Azure Resource Manager, as seguintes páginas são visíveis. Lembre-se de que as alterações que você faz se aplicam apenas às máquinas que você adiciona ao catálogo posteriormente. As máquinas existentes permanecem inalteradas.

- Na página **Máquinas Virtuais**, altere o tamanho da máquina e as zonas de disponibilidade onde você deseja criar máquinas.

  > **Nota:**
  >
  > - Somente os tamanhos de máquina compatíveis com o catálogo são exibidos.
  > - Se necessário, selecione **Mostrar apenas tamanhos de máquina usados em outros catálogos de máquinas** para filtrar a lista de tamanhos de máquina.

- Na página **Perfil da Máquina**, escolha se deseja usar ou alterar um perfil de máquina.
- (Visível apenas quando o catálogo está configurado com um host de grupo dedicado) Na página **Grupo de host dedicado**, escolha se deseja alterar um grupo de host.
- Na página **Tipos de Armazenamento e Licença**, escolha se deseja alterar o tipo de armazenamento, o tipo de licença e as configurações da Galeria de Computadores do Azure (disponível apenas quando **Colocar imagem preparada na Galeria do Azure** estiver em uso).

> **Nota:**
>
> Se a configuração recém-selecionada não suportar o tamanho atual da máquina, uma caixa de diálogo de aviso aparecerá, informando que a alteração da configuração redefine a configuração de tamanho da máquina. Se você optar por continuar, um ponto vermelho aparecerá ao lado do menu **Máquinas Virtuais**, solicitando que você selecione um novo tamanho de máquina.

- Na página **Tipo de Licença**, escolha se deseja alterar a configuração de licença do Windows ou licença do Linux.

Para catálogos de Acesso Remoto a PC, as seguintes páginas estão visíveis:

- Na página **Gerenciamento de Energia**, altere as configurações de gerenciamento de energia e selecione uma conexão de gerenciamento de energia.
- Na página **Unidades Organizacionais**, adicione ou remova UOs do Active Directory.

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 **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Renomear Catálogo de Máquinas** na barra de ações.
4. Insira o novo nome.

## Mover um catálogo para uma zona diferente

Se sua implantação tiver mais de uma zona, você poderá mover um catálogo de uma zona para outra.

Mover um catálogo para uma zona diferente, que não seja o hipervisor que contém as VMs nesse catálogo, afeta o desempenho.

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Mover** na barra de ações.
4. Selecione a zona para onde você deseja mover o catálogo.

## Excluir um catálogo

Antes de excluir um catálogo, certifique-se de que:

- Todos os usuários são desconectados e você não executa nenhuma sessão desconectada.
- O modo de manutenção está ativado para todas as máquinas no catálogo para que novas conexões não possam ser feitas.
- Todas as máquinas no catálogo estão desligadas.
- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Excluir Catálogo de Máquinas** na barra de ações.
4. Indique se as máquinas no catálogo são excluídas. Se você optar por excluir as máquinas, indique se as contas de computador do Active Directory para essas máquinas são retidas, desabilitadas ou excluídas.

## Gerenciar contas de computador do Active Directory em um catálogo

Para gerenciar contas do Active Directory em um catálogo de máquinas, você pode:

- Libere contas de máquina não utilizadas removendo contas de computador do Active Directory de catálogos de SO de sessão única e SO de várias sessões. Essas contas podem então ser usadas para outras máquinas.
- Adicionar contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam no lugar. Não use uma barra (/) em um nome de OU.

Para gerenciar contas do Active Directory:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Gerenciar contas AD** na barra de ações.
4. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas das contas: redefina todas elas ou insira uma senha que se aplique a todas as contas.

   Você pode redefinir senhas se não souber as senhas atuais da conta; você deve ter permissão para realizar uma redefinição de senha. Ao inserir uma senha, a senha é alterada nas contas à medida que são importadas. Ao excluir uma conta, escolha se a conta no Active Directory é mantida, desabilitada ou excluída.

Indique se as contas do Active Directory são retidas, desabilitadas ou excluídas ao remover máquinas de um catálogo ou excluir um catálogo.

## Atualizar um catálogo

Recomendamos que você salve cópias ou instantâneos de imagens mestre antes de atualizar as máquinas no catálogo. O banco de dados mantém um registro histórico das imagens mestre

usadas com cada catálogo de máquinas. Reverta, ou desfaça, as máquinas em um catálogo para usar a versão anterior da imagem mestre. Execute esta tarefa se os usuários encontrarem problemas com as atualizações que você implantou em seus desktops. Isso minimiza o tempo de inatividade do usuário. Não exclua, mova ou renomeie imagens mestre. Você não pode reverter um catálogo para usá-las.

Depois que uma máquina é atualizada, ela reinicia automaticamente.

### Atualizar ou criar uma imagem mestre

Antes de atualizar o catálogo de máquinas, atualize uma imagem mestre existente ou crie uma em seu hipervisor host.

1. No seu hipervisor, tire um instantâneo da VM atual e dê um nome significativo ao instantâneo. Este instantâneo pode ser usado para reverter (restaurar) máquinas no catálogo, se necessário.
2. Se necessário, ligue a imagem mestre e faça login.
3. Instale atualizações ou faça as alterações necessárias na imagem mestre.
4. Desligue a VM.
5. Tire um instantâneo da VM. Dê a ele um nome significativo que seja reconhecido quando o catálogo for atualizado no Web Studio. Embora o Web Studio possa criar um instantâneo, a Citrix recomenda que você o crie usando o console de gerenciamento do hipervisor. Em seguida, selecione esse instantâneo no Web Studio. Esse processo permite que você forneça um nome e uma descrição significativos, em vez de um nome gerado automaticamente. Para imagens mestre de GPU, você pode alterar a imagem mestre apenas através do console do XenServer®.

### Alterar a imagem mestre

Para preparar e implantar a atualização em todas as máquinas de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Alterar Imagem Mestre** na barra de ações.
4. Na página **Imagem**, selecione o host e a imagem que você deseja implantar.

> **Dica:**

> Para um catálogo criado por MCS, você pode anotar sua imagem adicionando uma nota para a imagem. Uma nota pode conter até 500 caracteres. Cada vez que você altera a imagem mestre, uma entrada relacionada à nota é criada, independentemente de você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como nula (-). Para visualizar o histórico de notas da imagem, selecione o catálogo, clique em **Propriedades do Modelo** no painel inferior e, em seguida, clique em **Exibir histórico de notas**.

5. Na página **Estratégia de Implantação**, escolha quando as máquinas no catálogo de máquinas serão atualizadas com a nova imagem mestre: no próximo desligamento ou imediatamente.

> **Observação:**
>
> A página **Estratégia de Implantação** não está disponível para VMs persistentes porque a implantação é aplicável apenas a VMs não persistentes.

6. Verifique as informações na página **Resumo** e clique em **Concluir**. Cada máquina é reiniciada automaticamente após ser atualizada.

Para acompanhar o progresso da atualização, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Ao atualizar um catálogo usando o PowerShell SDK diretamente, em vez do Web Studio, especifique um modelo de hipervisor (**VMTemplates**). Use isso como uma alternativa a uma imagem ou a um instantâneo de uma imagem.

**Estratégia de implantação:**

A atualização de imagens no próximo desligamento afetará imediatamente todas as máquinas que não estão em uso no momento, ou seja, máquinas que não possuem uma sessão de usuário ativa. Um sistema em uso recebe a atualização quando a sessão ativa atual termina. Considere o seguinte:

- Novas sessões não podem ser iniciadas até que a atualização seja concluída nas máquinas aplicáveis.
- Para máquinas de SO de sessão única, as máquinas são atualizadas imediatamente quando a máquina não está em uso ou quando os usuários não estão logados.

- Para um SO multi-sessão com máquinas filhas, as reinicializações não ocorrem automaticamente. Para aplicar a imagem mestre atualizada, reinicie as máquinas usando o Studio, PowerShell ou Workspace. A reinicialização a partir das máquinas ou do hipervisor não aplica a atualização.

> **Dica:**
>
> Limite o número de máquinas sendo reiniciadas usando as configurações avançadas para uma conexão de host. Use essas configurações para modificar as ações tomadas para um determinado catálogo; as configurações avançadas variam dependendo do hipervisor.

### Reverter a imagem mestre

Depois de implantar uma imagem mestre atualizada ou nova, você pode revertê-la. Esse processo pode ser necessário se ocorrerem problemas com as máquinas recém-atualizadas. Ao reverter, as máquinas no catálogo são revertidas para a última imagem funcional. Quaisquer novos recursos que exijam a imagem mais recente não estarão mais disponíveis. Assim como na implantação, reverter uma máquina inclui uma reinicialização.

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione o catálogo e, em seguida, selecione **Reverter Imagem Mestra** na barra de ações.
4. Especifique quando aplicar a imagem mestre anterior às máquinas, conforme descrito na seção anterior para a operação de implantação.

A reversão é aplicada apenas às máquinas que precisam ser revertidas. As máquinas que não são atualizadas com a imagem mestre nova ou atualizada não recebem mensagens de notificação e não são forçadas a fazer logoff.

Para acompanhar o progresso da reversão, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

## Alterar o nível funcional ou desfazer a alteração

Altere o nível funcional do catálogo de máquinas depois de atualizar os VDAs nas máquinas para uma versão mais recente. A Citrix recomenda atualizar todos os VDAs para a versão mais recente para permitir o acesso a todos os recursos mais recentes.

Antes de alterar o nível funcional para um catálogo de máquinas:

- Inicie as máquinas atualizadas para que elas se registrem no Controller. Esse processo permite que o Web Studio determine que as máquinas no catálogo precisam de atualização.

Para alterar o nível funcional de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione o catálogo. A guia **Detalhes** no painel inferior exibe as informações da versão.
4. Selecione **Alterar Nível Funcional**. Se o Web Studio detectar que o catálogo precisa de atualização, ele exibirá uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser atualizadas, uma mensagem explicará o motivo. Para garantir que todas as máquinas funcionem corretamente, a Citrix recomenda que você resolva os problemas da máquina antes de clicar em **Alterar** para prosseguir.

Após a conclusão da alteração do catálogo, você pode reverter as máquinas para suas versões VDA anteriores selecionando o catálogo e, em seguida, selecionando **Desfazer Alteração de Nível Funcional** na barra de ações.

## Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Você não pode alterar as configurações associadas ao sistema operacional e ao gerenciamento de máquinas. O catálogo clonado herda essas configurações do original.
- A clonagem de um catálogo pode levar algum tempo para ser concluída. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.
- O catálogo clonado herda o nome do original e tem o sufixo `Copy`. Você pode alterar o nome. Consulte Renomear um catálogo.
- Após a conclusão da clonagem, certifique-se de atribuir o catálogo clonado a um grupo de entrega.

1. Faça login no Web Studio e selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Clonar** na barra de ações.
3. Na janela **Clonar Catálogo de Máquinas Selecionado**, visualize as configurações do catálogo clonado e configure as configurações conforme aplicável. Selecione **Avançar** para prosseguir para a próxima página.
4. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para iniciar a clonagem.

5. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.

## Organizar catálogos usando pastas

Você pode criar pastas para organizar catálogos para facilitar o acesso. Por exemplo, você pode organizar catálogos por tipo de imagem ou por estrutura organizacional.

### Criar uma pasta de catálogo

Antes de começar, planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis de profundidade (excluindo a pasta raiz padrão).
- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós no Web Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça no nó **Catálogos de Máquinas**, você deve adicionar os metadados `ContainsMachineCatalogs` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

Para criar uma pasta de catálogo, siga estas etapas:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra de **Ações**.
3. Digite um nome para a nova pasta e clique em **Concluído**.

**Dica:**

Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

### Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Visualize catálogos por pasta. Você também pode ativar **Visualizar tudo** acima da hierarquia de pastas para visualizar todos os catálogos de uma vez.
3. Clique com o botão direito em um catálogo e selecione **Mover Catálogo de Máquinas**.
4. Selecione a pasta para a qual você deseja mover o catálogo e clique em **Concluído**.

> **Dica:**
>
> Você pode arrastar um catálogo para uma pasta.

### Gerenciar pastas de catálogo

Você pode excluir, renomear e mover pastas de catálogo.

Você pode excluir uma pasta somente se ela e suas subpastas não contiverem catálogos.

Para gerenciar uma pasta, siga as etapas abaixo:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

## Usar PowerShell

Esta seção detalha como você pode gerenciar catálogos usando o PowerShell:

- Recuperar avisos e erros associados a um catálogo
- Adicionar descrições a uma imagem
- Redefinir disco do SO

- Alterar a configuração de rede para um esquema de provisionamento existente
- Gerenciar versões de um catálogo de máquinas
- Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina
- Reparar as informações de identidade de contas de computador ativas
- Alterar a configuração de cache em um catálogo de máquinas existente
- Suporte à atualização do VDA via acesso a compartilhamento de arquivo local(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#vda-update-support-via-local-file-share-access)

## Recuperar avisos e erros associados a um catálogo

Você pode obter erros e avisos históricos para entender os problemas com seu catálogo de máquinas MCS e corrigi-los.

Usando comandos PowerShell, você pode:

- Obter uma lista de erros ou avisos
- Alterar o estado do aviso de **Novo** para **Reconhecido**
- Excluir os erros ou avisos

Para executar os comandos PowerShell:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

Para obter uma lista de erros e avisos:

Execute o comando `Get-ProvOperationEvent`.

- Sem parâmetros: Obtém todos os erros e avisos
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Obtém todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `EventId`: Obtém um erro ou aviso específico que corresponde a este ID de evento
- Com o parâmetro `Filter`: Obtém erros ou avisos por filtro personalizado

Para alterar o estado de erros ou avisos de **Novo** para **Reconhecido**:

Execute o comando `Confirm-ProvOperationEvent`.

- Com o parâmetro `EventId`: Define o estado de um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como uma saída do comando `Get-ProvOperationEvent`
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Define o estado de todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Define o estado de todos os erros e avisos como **Reconhecido**

Para excluir os erros ou avisos:

Execute o comando `Remove-ProvOperationEvent`.

- Com o parâmetro `EventId`: Remove um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como saída do comando `Get-ProvOperationEvent`.
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Remove todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Remove todos os erros e avisos

Para obter mais informações, consulte Citrix PowerShell SDK.

## Adicionar descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagem para catálogos de máquinas. Use este recurso para adicionar uma descrição ao criar um catálogo ou ao atualizar uma imagem mestre existente para um catálogo. Você também pode exibir informações para cada imagem mestre no catálogo. Use os seguintes comandos para adicionar ou visualizar descrições de imagem:

- Para adicionar uma nota ao criar um catálogo de máquinas com uma imagem mestre, use o parâmetro `MasterImageNote` no comando `NewProvScheme`. Por exemplo:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
<name> -IdentityPoolName <name> -MasterImageVM

XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
-MasterImageNote "Note"
```

- Para atualizar a imagem mestre associada a um catálogo de máquinas, use o parâmetro `MasterImageNote` no comando `Publish-ProvMasterVMImage`. Por exemplo:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
-MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
name>.vm\base.snapshot -MasterImageNote "Note"
```

- Para exibir as informações de cada imagem, use o comando Get-ProvSchemeMasterVMImageHistory. Por exemplo:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

Para acompanhar o progresso da reversão, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em certos cenários, incluindo os seguintes. (A opção **Reverter Imagem Mestra** não está visível).

- Você não tem permissão para reverter.
- O catálogo não foi criado usando o MCS.
- O catálogo foi criado usando uma imagem do disco do SO.
- O instantâneo usado para criar o catálogo foi corrompido.
- As alterações do usuário nas máquinas do catálogo não persistem.
- As máquinas no catálogo estão em execução.

## Redefinir disco do SO

Use o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado pelo MCS. Atualmente, esse recurso é aplicável a ambientes de virtualização AWS, Azure, XenServer, Google Cloud, SCVMM e VMware.

Para executar o comando PowerShell com sucesso, certifique-se de que:

- As VMs de destino estão em um catálogo MCS persistente.
- O catálogo de máquinas MCS está funcionando corretamente.
- Isso implica que o esquema de provisionamento e o host existem, e o esquema de provisionamento possui entradas corretas.

- O hipervisor não está em modo de manutenção.
- As VMs de destino estão desligadas e em modo de manutenção.

Execute as seguintes etapas para redefinir o disco do SO:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando PowerShell `Reset-ProvVMDisk` de uma das seguintes maneiras:

   - Especifique a lista de VMs como uma lista separada por vírgulas, e execute a redefinição em cada VM:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
     -OS
     ```

   - Especifique a lista de VMs como uma saída do comando `Get-ProvVM`, e execute a redefinição em cada VM:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
     -OS
     ```

   - Especifique uma única VM pelo nome:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     ```

   - Crie tarefas de redefinição separadas para cada uma das VMs retornadas pelo comando `Get-ProvVM`. Isso é menos eficiente porque cada tarefa executará as mesmas verificações redundantes, como verificação de capacidade do hipervisor, verificação de conexão para cada VM.

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
     -ProvisioningSchemeName "xxx" -OS
     ```

4. Um prompt de confirmação aparece listando as VMs a serem redefinidas, juntamente com uma mensagem de aviso de que é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma outra ação será executada.

   **Nota:**

> Não retire as VMs do modo de manutenção nem as ligue até a conclusão do processo de redefinição.

> Você pode executar o comando PowerShell `-WhatIf` para imprimir a ação que ele executaria e sair sem realizar a ação.

Você também pode ignorar o prompt de confirmação usando um dos seguintes métodos:

- Forneça o parâmetro `-Force`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- Forneça o parâmetro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- Antes de executar o `Reset-ProvVMDisk`, altere `$ConfirmPreference` para **None**:

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. Execute `Get-ProvTask` para obter o status das tarefas retornadas pelo comando `Reset-ProvVMDisk`.

## Alterar a configuração de rede para um esquema de provisionamento existente

Você pode alterar a configuração de rede para um esquema de provisionamento existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede.

> **Nota:**
>
> Este recurso é compatível com Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versões posteriores.

> Para alterar a configuração de rede para um esquema de provisionamento existente, faça o seguinte:

1. Na janela do PowerShell, execute o comando `asnp citrix*` para carregar os módulos do PowerShell.
2. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para acessar o caminho de rede que você deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

   ```
   $NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network"}
   ```

4. Execute `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`.
5. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar a nova configuração de rede para o esquema de provisionamento existente.

## Gerenciar versões de um catálogo de máquinas

Quando um catálogo de máquinas MCS é atualizado com o comando `Set-ProvScheme`, a configuração atual é salva como uma versão. Você pode então gerenciar as várias versões do catálogo de máquinas usando comandos do PowerShell. Você pode:

- Ver a lista de versões de um catálogo de máquinas
- Use qualquer versão anterior para atualizar o catálogo de máquinas
- Exclua manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas
- Altere o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99)

Uma versão inclui as seguintes informações de um catálogo de máquinas:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Execute os seguintes comandos (fornecidos como exemplos) para gerenciar as várias versões de um catálogo de máquinas.

- Para ver os detalhes de configuração das várias versões de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Para ver os detalhes de configuração de uma versão específica de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para ver o número total de versões associadas a um catálogo de máquinas:

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- Para usar qualquer versão anterior para atualizar o catálogo de máquinas:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para excluir manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- Para definir o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99). Essa configuração é aplicada a todos os catálogos. Por exemplo, neste caso, um máximo de 15 versões será retido para todos os catálogos provisionados por MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

Se o número de versões atingir o número máximo de versões, uma nova versão não poderá ser criada se versões mais antigas estiverem em uso por qualquer uma das VMs no catálogo de máquinas. Nesse caso, faça uma das seguintes ações:

- Aumente o limite do número máximo de versões a serem retidas pelo catálogo de máquinas.
- Atualize algumas VMs que estão em versões mais antigas para que essas versões mais antigas não sejam mais referenciadas por nenhuma VM e possam ser excluídas.

## Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina

Você pode usar uma VM, especificação de modelo (no caso do Azure) ou modelo de inicialização (no caso da AWS) como entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina. Novas VMs adicionadas ao catálogo assumem os valores de propriedade do perfil da máquina, a menos que sejam substituídos por uma propriedade personalizada explícita.

> **Nota:**
>
> Um catálogo de máquinas existente baseado em perfil de máquina não pode ser alterado para um catálogo de máquinas não baseado em perfil de máquina.

Para fazer isso:

1. Crie um catálogo de máquinas persistente ou não persistente com VMs e sem um perfil de máquina.
2. Abra a janela do **PowerShell**.
3. Execute o comando `Set-ProvScheme` para aplicar os valores de propriedade do perfil da máquina às novas VMs adicionadas ao catálogo de máquinas. Por exemplo:
    - No caso do Azure:

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
Name>\<TemplateSpecName>\<VersionName>
```

- No caso da AWS:

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
\HostingUnits\<hosting-unit>\<launch-
template>.launchtemplate\<launch-template-
version>.launchtemplateversion"
```

## Reparar as informações de identidade de contas de computador ativas

Você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

**Nota:**

Atualmente, o recurso é suportado apenas para ambientes de virtualização Azure e VMware.

### Condições

Certifique-se do seguinte para redefinir o disco de identidade com sucesso:

- Desligue e defina a VM para o modo de manutenção
- Não inclua o parâmetro -OS no comando PowerShell

### Redefinir disco de identidade

Para redefinir o disco de identidade:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Redefina as informações de identidade.
    - Para redefinir apenas a senha da máquina e as chaves de confiança, execute o seguinte comando:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

A descrição dos parâmetros usados no comando é a seguinte:

- IdentityAccountName: O nome da conta de identidade que deve ser reparada.
- PrivilegedUserName: Conta de usuário que tem permissão de gravação no provedor de identidade (AD ou AzureAD).
- PrivilegedUserPassword: Senha para PrivilegedUserName.
- Target: Destino para a ação de reparo. Pode ser IdentityInfo para reparar a senha da conta/chave de confiança, e UserCertificate para reparar os atributos do certificado de usuário de identidades de máquina unidas ao Hybrid AzureAD.

- Para redefinir toda a configuração do disco de identidade, execute os seguintes comandos na seguinte ordem:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- Para recriar completamente o disco de identidade:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. Digite **y** para confirmar a ação. Você também pode pular o prompt de confirmação usando o parâmetro `-Force`. Por exemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. Execute `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` para verificar a configuração atualizada do disco de identidade. Os atributos do disco de identidade (por

exemplo, `IdentityDiskId`) devem ser atualizados. O `StorageId` e o `IdentityDiskIndex` não devem ser alterados.

## Alterar a configuração do cache em um catálogo de máquinas existente

Após criar um catálogo não persistente com o MCSIO ativado, você pode usar o comando Set-ProvScheme para modificar os seguintes parâmetros:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Este recurso é atualmente aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO ativado

### Requisitos

Os requisitos para modificar a configuração do cache são:

- Atualize para a versão mais recente do VDA (2308 ou posterior).
- Habilite o parâmetro `UseWriteBackCache` para o catálogo de máquinas existente. Use `New-ProvScheme` para criar um catálogo de máquinas com `UseWriteBackCache` ativado. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

### Alterar a configuração do cache

Execute o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

**Nota:**

- O valor de `WriteBackCacheDiskSize` deve ser maior que zero, pois é necessário pelo menos 1 GB de armazenamento em disco de cache.
- O valor de `WriteBackCacheMemorySize` deve ser menor que o tamanho da memória do catálogo de máquinas.
- Essas alterações afetam apenas as novas VMs adicionadas ao catálogo após a alteração. As VMs existentes não são afetadas por essas alterações.

## Suporte à atualização do VDA via acesso a compartilhamento de arquivos local

Especifique o local do instalador do VDA por meio de cmdlets do PowerShell, o que reduz seu esforço de fornecer regras de rede para permitir que cada VDA vá e busque o novo instalador do VDA do Citrix Managed Azure CDN.

### Cmdlets do PowerShell

Dois novos parâmetros opcionais adicionados aos cmdlets **New-VusCatalogSchedule** e **New-VusMachineUpgrade** que permitem usar instaladores de um compartilhamento de arquivos local

- **VdaWorkstationPackageUri** - para especificar o caminho UNC para o instalador VDA do SO da estação de trabalho
- **VdaServerPackageUri** - para especificar o caminho UNC para o instalador VDA do SO do servidor

### Pré-requisitos

- Instalador do Agente VUS que acompanha o VDA 2311
- Agente de atualização do VDA para a versão 7.40.0.35 ou posterior (usando o instalador do VDA versão 2311 ou posterior)

- SDK do PowerShell Remoto do Virtual Apps and Desktops versão 7.40 ou mais recente (lançado em Jan 10, 2024 ou posterior)

### Como Definir Permissões de Compartilhamento de Arquivos

Os compartilhamentos de rede que contêm pacotes de instalação VDA devem ter acesso de leitura para o serviço do Agente de Atualização VDA, que é executado como Sistema Local (principal NT AUTHORITY\SYSTEM).

- **Permissão de compartilhamento de arquivo associado ao domínio**

  Quando a máquina VDA está associada ao domínio, a conta **Sistema Local** (o VUA é executado como Sistema Local) usa credenciais de computador ao acessar compartilhamentos de rede.

  A permissão de privilégio mínimo pode ser definida concedendo acesso de **Leitura** aos Computadores de Domínio.

  a. Escolha as pessoas em sua rede com quem você deseja compartilhar o arquivo.
  b. Clique em **Configurações de Compartilhamento Avançadas** e ative o **Compartilhamento de Arquivos e Impressoras**.

- **Permissão de compartilhamento de arquivo não associado ao domínio**

  Quando a máquina VDA não está associada ao domínio, a conta **Sistema Local** (VUA é executado como Sistema Local) usa **LOGON ANÔNIMO** ao acessar compartilhamentos de rede.

  a. Selecione uma pasta compartilhada.
  b. Desative a proteção por senha.
     a. Vá para **Propriedades** da Pasta.
     b. Selecione **Central de Rede e Compartilhamento**.
     c. Desative o **Compartilhamento Protegido por Senha**.
  c. Clique em **Compartilhamento Avançado** para conceder uma permissão de compartilhamento.
     a. Selecione **Permissões**.
     b. Conceda uma permissão de compartilhamento de **Leitura** para **LOGON ANÔNIMO**.
  d. Selecione a **Guia Segurança** para conceder permissões de pasta

a. Clique em **Editar** para adicionar permissões à pasta compartilhada

b. Selecione a pasta compartilhada para conceder permissões de pasta a **ANONYMOUS LOGON**.

e. Clique em **Avançado** para ativar o **Compartilhamento de Arquivos e Impressoras**.

f. Adicione o nome da pasta compartilhada à **Política de Segurança de Acesso à Rede**.

> **Nota:**
>
> Reinicie sua máquina para que a alteração entre em vigor imediatamente.

### Atualizações do VDA a partir de um Compartilhamento de Arquivos Local

1. Baixe o instalador do VDA e coloque-o no arquivo compartilhado.

> **Nota:**
>
> Com o Serviço de Atualização Virtual, você pode selecionar entre a trilha de Versão Atual ou a trilha LTSR.
>
> **Por Exemplo:** Se o catálogo de máquinas estiver definido como Versão Atual, que é 2311, e a versão do VDA for 2305, você deve atualizar o VDA para a versão 2311.

a. navegar para a página **Downloads** em nosso site.

b. Selecione **Citrix Virtual Apps and Desktops** como o produto.

c. Selecione **Citrix Virtual Apps and Desktops 7 2311, Todas as Edições**.

d. Selecione o instalador do VDA em **Componentes que estão na ISO do produto, mas também são empacotados separadamente** (expansível).

2. Selecione o instalador do VDA relevante com base no tipo de catálogo.

- Baixe o **instalador do VDA do SO multi-sessão** se o tipo de catálogo for **multi-sessão**
- Baixe o **instalador do VDA do SO de sessão única** se o tipo de catálogo for **sessão única**

- Baixe o **Single-session OS Core Services VDA installer** se o tipo de catálogo for **Remote PC Access**

> **Nota:**
>
> A versão do instalador de compartilhamento de arquivos deve corresponder **exatamente** à versão do instalador mais recente publicada pela VUS na nuvem.

## Solução de problemas

- Para máquinas com status de "Estado de Energia Desconhecido", consulte CTX131267 para obter orientação.
- Para corrigir VMs que exibem continuamente um estado de energia desconhecido, consulte Como corrigir VMs que exibem continuamente um estado de energia desconhecido.

## Próximos passos

Para obter informações sobre como gerenciar catálogos de serviços de nuvem específicos, consulte:

- Gerenciar um catálogo AWS
- Gerenciar um catálogo do XenServer
- Gerenciar um catálogo do Google Cloud Platform
- Gerenciar um catálogo do Microsoft Azure
- Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager
- Gerenciar um catálogo do VMware

## Gerenciar um catálogo AWS

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem AWS.

> **Observação:**
>
> Antes de gerenciar um catálogo AWS, você precisa terminar de criar um catálogo AWS. Consulte Criar um catálogo AWS.

### Remover tags

Ao criar um catálogo ou uma VM, as tags criadas pelo MCS são criadas nos seguintes recursos:

- Máquina virtual
- Volume de disco raiz
- Volume de disco de identidade
- NIC
- Imagem de disco raiz (AMI)
- Modelo de inicialização
- Snapshot de AMI ou disco raiz

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix® e remover as tags criadas pelo MCS. Você pode usar:

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

Este recurso é aplicável apenas a VMs persistentes.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Desbloqueie a VM antes de remover as VMs. Por exemplo:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. Execute um dos seguintes comandos para remover VMs, catálogo de máquinas e tags criadas pelo MCS dos recursos.

   - Execute `Remove-ProvVM` com `ForgetVM` para remover VMs do banco de dados Citrix e tags das VMs. Por exemplo:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

- Execute `Remove-ProvScheme` para remover o catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas. Por exemplo:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. Verifique se a VM foi removida do Delivery Controller™, no entanto, não do hipervisor.

   a. Execute `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. Isso não deve retornar nada.

   b. Vá para o console AWS EC2. Você deve ver as VMs, no entanto, as tags foram removidas. As tags dos seguintes recursos são removidas:

      - Máquina virtual
      - Volume de disco raiz
      - Volume de disco de identidade
      - NIC

6. Se você remover o catálogo de máquinas, verifique se o catálogo foi removido do Delivery Controller.

   a. Execute `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Isso deve retornar um erro.

   b. Verifique no console do AWS EC2 se os seguintes recursos foram removidos.

      - Imagem do disco raiz (AMI)
      - Modelo de inicialização
      - Snapshot de AMI ou disco raiz

### Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

| NOME DO RECURSO | TAG |
|---|---|
| Disco de ID | "Name": "VMName_IdentityDisk" |
| | "XdConfig": "XdProvisioned=true" |

| NOME DO RECURSO | TAG |
|---|---|
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Imagem | "XdConfig": "XdProvisioned=true" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| NIC | "Descrição": "XD NIC" |
| | "XdConfig": "XdProvisioned=true" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco do SO | "Nome": "VMName_rootDisk" |
| | "XdConfig": "XdProvisioned=True" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | [when AwsCaptureInstanceProperties = true] "Recurso Citrix": "" |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": "" |
| PrepVM | "Nome": "Preparação - Nome do Catálogo - xxxxxxxxxx" |
| | "XdConfig": "XdProvisioned=true" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | [when AwsCaptureInstanceProperties = true] "Recurso Citrix": "" |

| NOME DO RECURSO | TAG |
|---|---|
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": "" |
| Instantâneo publicado | "XdConfig": "XdProvisioned=true" |
| | Se não for um snapshot para Volume Worker AMI, então "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Modelo | [when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true" |
| | [when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | [when AwsCaptureInstanceProperties = true] "Recurso Citrix": "" |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "Recurso Operacional Citrix": "" |
| VM no catálogo | "XdConfig": "XdProvisioned=true" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | [when AwsCaptureInstanceProperties = true] "CitrixResource": "" |
| | [when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx" |
| | [when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n" |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": "" |

| NOME DO RECURSO | TAG |
|---|---|
| AMI do worker de volume | "XdConfig": "XdProvisioned=true" |
| Inicializador de volume worker | "Name": "XenDesktop® Temp" |
| | "XdConfig": "XdProvisioned=true" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": "" |
| Instância de volume worker | "Nome": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx" |
| | "XdConfig": "XdProvisioned=true" |

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com a AWS
- Criar catálogos de máquinas
- Criar um catálogo da AWS
- Gerenciar catálogos de máquinas

## Gerenciar um catálogo XenServer®

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização XenServer.

> **Nota:**
>
> Antes de gerenciar um catálogo XenServer, você precisa terminar de criar um catálogo XenServer. Consulte Criar um catálogo XenServer.

### Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

| NOME DO RECURSO | TAG |
|---|---|
| Disco base publicado e sua cópia em cada rede ou armazenamento local | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco de ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco do SO | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| VM de Preparação | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| VM no catálogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco WBC | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com XenServer
- Criar catálogos de máquinas
- Criar um catálogo do XenServer
- Gerenciar catálogos de máquinas

## Gerenciar um catálogo do Google Cloud Platform

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes do Google Cloud.

> **Observação:**

> Antes de gerenciar um catálogo do Google Cloud Platform, você precisa concluir a criação de um catálogo do Google Cloud Platform. Consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html).

## Gerenciar catálogo de máquinas

Para adicionar máquinas a um catálogo, atualizar máquinas e reverter uma atualização, consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html).

## Gerenciamento de energia

O Citrix DaaS™ permite o gerenciamento de energia de máquinas do Google Cloud. Use o nó **Pesquisar** no painel esquerdo para localizar a máquina que você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Excluir
- Iniciar
- Reiniciar
- Reinicialização Forçada
- Desligar
- Desligamento Forçado
- Adicionar ao Grupo de Entrega
- Gerenciar Tags
- Ativar Modo de Manutenção

Você também pode gerenciar a energia das máquinas do Google Cloud usando o Autoscale. Para fazer isso, adicione as máquinas do Google Cloud a um Grupo de Entrega e, em seguida, habilite o Autoscale para esse Grupo de Entrega. Para obter mais informações sobre o Autoscale, consulte (/pt-br/citrix-daas/manage-deployment/autoscale.html).

### Atualizar máquinas provisionadas usando PowerShell

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, agora você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas persistentes ou não persistentes existentes. Atualmente, no GCP, a atualização de propriedade suportada por esse recurso é o perfil da máquina.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento

Para atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. Atualize o esquema de provisionamento. Por exemplo,

   ```
   `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
   "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
   ```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. Atualizar máquinas existentes.

   - Para atualizar todas as máquinas existentes:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar uma lista de máquinas específicas:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Para atualizar máquinas com base na saída de `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. Reinicie as máquinas. No próximo ligamento, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

### Alterar propriedades personalizadas relacionadas ao disco de um catálogo existente

Você pode alterar as seguintes propriedades personalizadas relacionadas ao disco de um catálogo existente e de VMs existentes do catálogo:

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

**Observação:**

- A propriedade `StorageType` é para o disco do SO

- A propriedade `PersistOsDisk` pode ser definida apenas para catálogos não persistentes com cache de write-back ativado

Esta implementação ajuda você a selecionar diferentes tipos de armazenamento para diferentes discos mesmo após a criação de um catálogo e, assim, equilibrar os preços associados a diferentes tipos de armazenamento.

Para fazer isso, use os comandos do PowerShell `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute `Get-ProvVM -VMName <VM name>` para obter as propriedades personalizadas.
4. Altere a string de propriedades personalizadas:
   a. Copie as propriedades personalizadas para um Bloco de Notas e altere as propriedades personalizadas.
   b. Na janela do **PowerShell**, cole as propriedades personalizadas modificadas do Bloco de Notas e atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />
```

```
</CustomProperties>'
```

5. Atualize o catálogo existente. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. Atualize as VMs existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. Reinicie as VMs. No próximo ligamento, as alterações de propriedade personalizadas são aplicadas às VMs existentes.

### Proteger a exclusão acidental de máquinas

O Citrix DaaS permite proteger os recursos do MCS no Google Cloud para evitar exclusões acidentais. Configure a VM provisionada definindo o sinalizador `deletionProtection` como TRUE.

Por padrão, as VMs provisionadas por meio do MCS ou do plug-in do Google Cloud são criadas com a proteção de instância ativada. A implementação é aplicável a catálogos persistentes e não persistentes. Os catálogos não persistentes são atualizados quando as instâncias são recriadas a partir do modelo. Para máquinas persistentes existentes, você pode definir o sinalizador no console do Google Cloud. Para obter mais informações sobre como definir o sinalizador, consulte o site da Documentação do Google. Novas máquinas adicionadas a catálogos persistentes são criadas com `deletionProtection` ativado.

Se você tentar excluir uma instância de VM para a qual definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você tiver a permissão `compute.instances.setDeletionProtection` ou a função IAM de **Administrador de Computação** atribuída, poderá redefinir o sinalizador para permitir que o recurso seja excluído.

### Identificar recursos criados por MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

| NOME DO RECURSO | TAG |
|---|---|
| Disco de ID | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Imagem | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco do SO | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| PrepVM | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Instantâneo publicado | "CitrixResource": "interno" |
| Bucket de armazenamento | "Citrixresource": "interno" |
| Modelo | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| VM no catálogo | "CitrixResource": "interno" |
| | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". O plug-in também adiciona este rótulo para VMs provisionadas pelo MCS: "citrix-provisioning-scheme-id": "provSchemeId". Você pode usar este rótulo para filtrar por catálogo no console do GCP. |
| Disco WBC | "CitrixResource": "interno" |
| | CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

> **Observação:**
>
> Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas
- Criar um catálogo Google Cloud Platform
- Gerenciar catálogos de máquinas

## Gerenciar um catálogo HPE Moonshot

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos do catálogo HPE Moonshot.

> **Nota:**
>
> Antes de gerenciar um catálogo HPE Moonshot, você precisa terminar de criar um catálogo HPE Moonshot.

### Gerenciamento de energia

O Citrix Virtual Apps and Desktops™ permite que você faça o gerenciamento de energia de máquinas HPE Moonshot. Use o nó **Pesquisar** no painel de navegação para localizar a máquina que você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Iniciar
- Desligar
- Desligamento Forçado
- Reiniciar

- Redefinir

> **Nota:**
>
> As ações de energia **Suspender** e **Retomar** não são suportadas.

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o HPE Moonshot
- Criar catálogos de máquinas
- Criar um catálogo de máquinas HPE Moonshot
- Gerenciar catálogos de máquinas

## Gerenciar um catálogo do Microsoft Azure

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

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de gerenciar um catálogo do Microsoft Azure, você precisa concluir a criação de um catálogo do Microsoft Azure. Consulte Criar um catálogo do Microsoft Azure.

### Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada

Você pode economizar custos de armazenamento alterando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade personalizada `StorageTypeAtShutdown`.

O tipo de armazenamento do disco muda para um nível inferior (conforme especificado na propriedade personalizada `StorageTypeAtShutdown`) quando você desliga a VM. Depois de ligar a VM, o tipo de armazenamento volta ao original (conforme especificado na propriedade personalizada `StorageType` ou na propriedade personalizada `WBCDiskStorageType`).

> **Importante:**
>
> O disco não existe até que a VM seja ligada pelo menos uma vez. Portanto, você não pode alterar o tipo de armazenamento ao ligar a VM pela primeira vez.

#### Requisitos

- Aplicável a um disco gerenciado. Isso implica que você define a propriedade personalizada `UseManagedDisks` como true.
- Aplicável a um catálogo persistente e não persistente com um disco de SO persistente. Isso implica que você define a propriedade personalizada `persistOsDisk` como true.
- Aplicável a um catálogo não persistente com um disco WBC persistente. Isso implica que você define a propriedade personalizada `persistWBC` como true.

#### Restrição

- De acordo com a Microsoft, você só pode alterar o tipo de disco duas vezes por dia. Consulte o documento da Microsoft. De acordo com a Citrix, a atualização `StorageType` ocorre sempre que há uma ação de Iniciar ou Desalocar para a VM. Portanto, limite o número de ações de energia por VM a duas por dia. Por exemplo, uma ação de energia pela manhã para iniciar a VM e uma à noite para desalocar a VM.

#### Alterar o tipo de armazenamento para um nível inferior

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

1. Adicione a propriedade personalizada `StorageTypeAtShutdown`, defina o valor como Standard_LRS (HDD) e crie um catálogo usando `New-ProvScheme`. Para obter informações sobre como criar um catálogo usando o PowerShell, consulte `<https://developer-`

`docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

**Nota:**

Se `StorageTypeAtShutdown` tiver qualquer valor diferente de vazio ou Standard_LRS (HDD), a operação falha.

Exemplo de configuração de propriedades personalizadas ao criar um catálogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

Exemplo de configuração de propriedades personalizadas ao criar um catálogo não persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

**Nota:**

Ao usar um perfil de máquina, a propriedade personalizada tem precedência sobre a propriedade definida em `MachineProfile`.

2. Desligue a VM e verifique o tipo de armazenamento da VM no portal do Azure. O tipo de armazenamento do disco muda para um nível inferior, conforme especificado na propriedade personalizada `StorageTypeAtShutdown`.

3. Ligue a VM. O tipo de armazenamento do disco volta para o tipo de armazenamento mencionado em:
    - propriedade personalizada `StorageType` para disco do SO
    - propriedade personalizada `WBCDiskStorageType` para disco WBC somente se você especificá-lo em `CustomProperties`. Caso contrário, ele volta para o tipo de armazenamento mencionado em `StorageType`.

**Aplicar `StorageTypeAtShutdown` a um catálogo existente**

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

Use `Set-ProvScheme` para adicionar uma VM a um catálogo existente. O recurso se aplica a novas VMs adicionadas após a execução de `Set-ProvScheme`. As máquinas existentes não são afetadas.

Exemplo de como definir propriedades personalizadas ao adicionar uma VM a um catálogo existente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
```

```
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

**Altere o tipo de armazenamento de VMs existentes para um nível inferior no desligamento**

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

Você pode economizar custos de armazenamento alterando o tipo de armazenamento das VMs existentes para um nível inferior quando as VMs são desligadas. Para fazer isso, use a propriedade personalizada `StorageTypeAtShutdown`.

Para alterar o tipo de armazenamento de máquinas existentes em um catálogo para um nível inferior quando as VMs são desligadas:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Altere a string de propriedades personalizadas.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. Atualize o esquema de provisionamento do catálogo existente. A atualização se aplica a novas VMs adicionadas após a execução de `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. Atualize as VMs existentes para habilitar `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. Na próxima vez que você ligar as máquinas, a propriedade `StorageTypeAtShutdown` das máquinas será atualizada. O tipo de armazenamento muda no próximo desligamento.
8. Execute o seguinte comando para visualizar o valor `StorageTypeAtShutdown` para cada VM em um catálogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

### Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas existente, persistente ou não persistente. Você também pode agendar um período de tempo para as atualizações de configuração das máquinas provisionadas pelo MCS existentes. Qualquer inicialização ou reinicialização durante o período de tempo agendado aplica uma atualização de esquema de provisionamento agendada a uma máquina. Atualmente, no Azure, você pode atualizar `ServiceOffering`, `MachineProfile` e as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

**Nota:**

- Você só pode atualizar as propriedades personalizadas `StorageType`, `WBCDiskStorageType` e `IdentityDiskStorageType` para um catálogo usando disco gerenciado em ambientes Azure.
- Se você executar `Set-ProvVMUpdateTimeWindow` duas vezes, o comando mais recente terá efeito.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento (nome do catálogo de máquinas)

Depois de fazer as seguintes alterações no esquema de provisionamento, a instância da VM é recriada para catálogos persistentes no Azure:

- Alterar o `MachineProfile`
- Remover `LicenseType`
- Remover `DedicatedHostGroupId`

**Nota:**

O disco do SO das máquinas existentes, juntamente com todos os seus dados, permanece como está e uma nova VM é anexada ao disco.

> Antes de atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. Atualize o esquema de provisionamento. Por exemplo,

   - Com a VM como entrada de perfil de máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - Com a especificação de modelo como entrada de perfil de máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<template-spec>.templatespec\<template-spec-
     version>.templatespecversion"

     -ServiceOffering "XDHyp:\HostingUnits\<hosting-
     unit>\serviceoffering.folder\<service-offering>.serviceoffering"
     ```

   - Apenas com a oferta de serviço:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
     "XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
     offering>.serviceoffering"
     ```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

Para solicitar atualizações para máquinas existentes que serão aplicadas na próxima reinicialização:

1. Execute os seguintes comandos para atualizar as máquinas existentes e fazer com que as atualizações sejam aplicadas na próxima reinicialização.
   - Para atualizar todas as máquinas existentes. Por exemplo,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar uma lista de máquinas específicas. Por exemplo,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar máquinas com base na saída de Get-ProvVM. Por exemplo,

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

**Nota:**

- `StartsNow` indica que a hora de início agendada é a hora atual.
- `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Reinicie as máquinas. No próximo ligamento, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Para agendar uma VM para atualizar para as configurações de provisionamento mais recentes na próxima vez que ela iniciar na janela de tempo agendada:

1. Execute os seguintes comandos:

   - Para agendar uma atualização com a hora de início como a hora atual

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -VMName vm1 -StartsNow -DurationInMinutes 120
   ```

   - Para agendar uma atualização em um fim de semana

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
   -VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
   (New –TimeSpan –Days 2).TotalMinutes
   ```

**Nota:**

- `VMName` é opcional. Se não for especificado, a atualização é agendada para todo o catálogo.
- Em vez de `StartTimeInUTC`, use `StartsNow` para indicar que a hora de início do agendamento é a hora atual.
- `DurationInMinutes` é opcional. O padrão é 120 minutos. Um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Verifique o status da atualização.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. Ligue a VM. Se você ligar a máquina após o período agendado, a atualização da configuração não será aplicada. Se você ligar a máquina dentro do período agendado,
    - Se a máquina estiver desligada e
        - você não liga a máquina, a atualização de configuração não é aplicada
        - você liga a máquina, a atualização de configuração é aplicada
    - Se a máquina estiver ligada e
        - você não reinicia a máquina, a atualização da configuração não é aplicada
        - você reinicia a máquina, a atualização da configuração é aplicada

Para cancelar a atualização da configuração:

Você também pode cancelar uma atualização de configuração de uma única VM, de várias VMs ou de um catálogo inteiro. Para cancelar uma atualização de configuração:

1. Execute `Clear-ProvVMUpdateTimeWindow`. Por exemplo:
    - Para cancelar a atualização da configuração agendada para uma única VM:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
    -VMName “vm1”
    ```

    - Para cancelar a atualização da configuração agendada para várias VMs:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
    -VMName "vm1","vm2"
    ```

    **Nota:**

    As VMs devem ser do mesmo catálogo.

### Atualizar propriedades de VMs individuais

Você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistente usando o comando PowerShell `Set-ProvVM`. No entanto, as atualizações não são aplicadas imediatamente. Você deve definir a janela de tempo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow` para que as atualizações sejam aplicadas.

Esta implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, este recurso é aplicável apenas ao ambiente Azure.

Atualmente, as propriedades que você pode atualizar são:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Usando este recurso, você pode:

- Atualizar as propriedades de uma VM
- Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas
- Reverter as atualizações de configuração aplicadas a uma VM

Antes de atualizar as propriedades de uma VM:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Verifique a configuração do catálogo de máquinas existente. Por exemplo:

   ```
   Get-ProvScheme -ProvisioningSchemeName AzureCatalog
   ```

4. Verifique a configuração da VM na qual você deseja aplicar as atualizações. Por exemplo:

   ```
   Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
   ```

#### Atualizar propriedades de uma VM

Faça o seguinte para atualizar as propriedades em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.

2. Atualize as propriedades da VM. Por exemplo, se você quiser atualizar a propriedade personalizada do tipo de armazenamento (`StorageType`) da VM, execute o seguinte:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

   Você pode atualizar as propriedades de duas VMs em um catálogo de máquinas simultaneamente. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

   **Observação:**

   As atualizações não são aplicadas imediatamente.

3. Obtenha a lista de propriedades que devem ser atualizadas e a versão da configuração. Por exemplo:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

   Verifique o valor da propriedade de `Version` e as propriedades a serem atualizadas (neste caso, `StorageType`).

4. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização ainda não foi aplicada. A VM ainda está na configuração antiga.

5. Solicite a atualização agendada. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

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

> **Observação:**
>
> Qualquer atualização pendente do esquema de provisionamento também é aplicada.

6. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização agora foi aplicada. A VM agora tem a nova configuração.

8. Para aplicar mais atualizações de configuração na VM, desligue a VM e repita os passos.

### Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas

Faça o seguinte para manter as propriedades atualizadas em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.
2. Atualize o catálogo de máquinas. Por exemplo, se você quiser alterar o tamanho da VM (`ServiceOffering`) e o tipo de armazenamento (`StorageType`), execute o seguinte:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. Obtenha os detalhes de configuração do catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

O `ProvisioningSchemeVersion` agora é incrementado em um. O tamanho da VM e o tipo de armazenamento também são atualizados.

4. Atualize as propriedades da VM. Por exemplo, forneça um perfil de máquina para a VM.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **Observação:**
>
> A entrada do perfil da máquina tem uma tag e um tamanho de VM diferente (`ServiceOffering`) especificado.

5. Obtenha a lista de propriedades que a VM terá após mesclar as atualizações de configuração na VM com as atualizações do catálogo de máquinas. Por exemplo:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **Observação:**
>
> Quaisquer atualizações na VM substituirão as atualizações feitas no catálogo de máquinas.

6. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

A VM mantém seu tamanho de VM atualizado conforme derivado do perfil da máquina. Os valores de tag especificados no perfil da máquina também são aplicados à VM. No entanto, o tipo de armazenamento é derivado do esquema de provisionamento mais recente.

8. Obtenha a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

O `ProvisioningSchemeVersion` e o `ProvVMConfigurationVersion` agora mostram a versão mais recente.

**Reverter as atualizações de configuração aplicadas a uma VM**

1. Após aplicar as atualizações a uma VM, desligue a VM.
2. Execute o seguinte comando para remover as atualizações aplicadas na VM. Por exemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Verifique a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

O valor `ProvVMConfigurationVersion` agora é a versão de configuração do catálogo de máquinas.

### Recuperar informações para VMs do Azure, snapshots, disco do SO e definição de imagem da galeria

Você pode exibir informações para uma VM do Azure, incluindo disco e tipo de SO, instantâneo e definição de imagem da galeria. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Use essa funcionalidade para visualizar e selecionar uma imagem Linux ou Windows. Uma propriedade do PowerShell, `TemplateIsWindowsTemplate`, foi adicionada ao parâmetro `AdditionDatafield`. Este campo contém informações específicas do Azure: tipo de VM, disco do SO, informações da imagem da galeria e informações do tipo de SO. Definir `TemplateIsWindowsTemplate` como **True** indica que o tipo de SO é Windows; definir `TemplateIsWindowsTemplate` como **False** indica que o tipo de SO é Linux.

> **Dica:**
>
> As informações exibidas pela propriedade PowerShell `TemplateIsWindowsTemplate` são derivadas da API do Azure. Às vezes, este campo pode estar vazio. Por exemplo, um snapshot de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de SO não pode ser recuperado de um snapshot.

Por exemplo, defina o parâmetro `AdditionData` da VM do Azure como **True** para o tipo de SO Windows usando o PowerShell:

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2
```

```
TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

### Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

| NOME DO RECURSO | TAG |
|---|---|
| Disco de ID | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| Imagem | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| NIC | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| Disco do SO | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| PrepVM | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| Instantâneo publicado | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |

| NOME DO RECURSO | TAG |
|---|---|
| Grupo de recursos | "CitrixResource" : "Internal" |
| | CitrixSchemaVersion: 2.0 |
| | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Conta de armazenamento | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| VM no catálogo | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |
| Disco WBC | "CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "CitrixResource" : "Internal" |

**Nota:**

Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure
- Criar catálogos de máquinas
- Criar um catálogo do Microsoft Azure
- Gerenciar catálogos de máquinas

# Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

**Observação:**

Antes de gerenciar um catálogo VMM, você precisa terminar de criar um catálogo VMM. Consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager.

## Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "chave":"valor".

| NOME DO RECURSO | TAG |
|---|---|
| VM de Preparo | String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True" |
| VM no catálogo | String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True" |

## Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas
- Criar um catálogo Microsoft System Center Virtual Machine Manager
- Gerenciar catálogos de máquinas

# Gerenciar um catálogo VMware

(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

> **Nota:**
>
> Antes de gerenciar um catálogo VMware, você precisa terminar de criar um catálogo VMware. Consulte Criar um catálogo VMware.

## Atualizar o ID da pasta de um catálogo de máquinas

Você pode atualizar o ID da pasta de um catálogo de máquinas MCS especificando o `FolderId` nas propriedades personalizadas do comando `Set-ProvScheme`. As VMs criadas após a atualização do ID da pasta são criadas sob este novo ID de pasta. Se esta propriedade não for especificada em `CustomProperties`, as VMs serão criadas na pasta onde a imagem mestre está localizada.

Execute as seguintes etapas para atualizar o ID da pasta de um catálogo de máquinas.

1. Abra um navegador da Web e insira o URL para o **vSphere Web Client**.
2. Insira as credenciais e clique em **Login**.
3. Crie uma pasta de posicionamento de VM no **vSphere Web Client**.
4. Abra uma janela do PowerShell.
5. Execute **asnp citrix®*** para carregar os módulos PowerShell específicos da Citrix.
6. Especifique o `FolderID` no `CustomProperties` de `Set-ProvScheme`. Neste exemplo, o valor do ID da pasta é `group-v2406`.

   ```
   Set-ProvScheme -ProvisioningSchemeUid
   "50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
   "<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
   machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
   instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
   Value=""group-v2406"" /></CustomProperties>"
   ```

7. Adicione uma VM ao catálogo de máquinas usando o Studio.
8. Verifique a nova VM no vSphere Web Client. A nova VM é criada na nova pasta.

### Encontrar o ID da pasta no vSphere

Acesse o Managed Object Browser (MOB) em qualquer sistema de servidor ESXi ou vCenter para encontrar o ID da pasta das VMs.

O MOB é um aplicativo de servidor baseado na web disponível embutido em todos os sistemas de servidor ESX/ESXi e vCenter. Este utilitário do vSphere permite visualizar informações detalhadas sobre objetos como VMs, datastores e pools de recursos.

1. Abra um navegador da web e insira `http://x.x.x.x/mob`, onde x.x.x.x é o endereço IP do vCenter Server ou host ESX/ESXi. Por exemplo, `<https://10.60.4.70/mob>`.
2. Na página **Home** do MOB, clique no valor da propriedade **content**.
3. Clique no valor de **rootFolder**.
4. Clique no valor de **childEntity**.
5. Clique no valor de **vmFolder**.
6. Você pode encontrar o ID da pasta no valor de **childEntity**.

## Migração de armazenamento de VMs

Você pode mover o armazenamento em disco de VMs existentes de um armazenamento antigo para um novo armazenamento. Durante a migração, o MCS mantém os recursos da VM, como gerenciamento de energia, redefinição do disco do SO e assim por diante. Você também pode adicionar novas VMs ao catálogo de máquinas usando o novo armazenamento em disco. Para fazer isso, use o comando PowerShell `Move-ProvVMDisk`.

Atualmente, você só pode migrar VMs persistentes de clone completo.

O novo armazenamento deve satisfazer as seguintes condições:

- Deve estar dentro do mesmo cluster do armazenamento antigo.
- O host no qual a VM está sendo executada deve ter acesso aos datastores antigo e novo.

Você pode realizar as seguintes tarefas:

- Migrar o armazenamento em disco
- Descontinuar o armazenamento antigo

### Migrar o armazenamento em disco

Para migrar o armazenamento em disco:

1. Adicione um novo armazenamento a uma unidade de hospedagem existente. Altere o armazenamento antigo para **Substituído**. Você pode fazer isso usando o Web Studio ou comandos PowerShell.

   - Se estiver usando o Web Studio, consulte Editar armazenamento.
   - Se estiver usando comandos PowerShell:

     - Execute `Add-Hyphostingunitstorage` para adicionar o novo armazenamento à unidade de hospedagem existente.
     - Execute `Set-Hyphostingunitstorage` com **Superseded** como true para desabilitar a criação de novas VMs no armazenamento antigo.

2. Desligue as VMs e ative o **Modo de Manutenção**.
3. Mova o armazenamento em disco das VMs para o novo armazenamento e atualize as informações de armazenamento. Por exemplo:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. Obtenha o ID da tarefa da migração. Por exemplo:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. Verifique o status da migração.

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: Fornece a lista de VMs com migração de disco bem-sucedida, incluindo as VMs que já foram migradas para o novo armazenamento.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: Fornece a lista de VMs com migração falha.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: Fornece a lista de VMs cuja migração ainda não foi iniciada.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: Fornece as propriedades atualizadas da VM após a migração. Verifique as propriedades como

`StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` e `LastBootTime`.

Após migrar os discos de VMs criadas pelo MCS com snapshot, você pode ver o aviso **Consolidation is required in the VSphere Client**. Para consolidar e evitar perda de dados:

1. Faça um backup da VM VMware. Por exemplo, transfira todos os arquivos da VM para outra pasta em um datastore.
2. Depois de ver o aviso, clique em **Consolidate** e, em seguida, clique em **OK** para confirmar a consolidação.

#### Descontinuar o armazenamento antigo

Para descontinuar o armazenamento antigo após a migração de disco das VMs:

1. Obtenha as informações sobre os discos base e a contagem de máquinas em cada armazenamento de disco da unidade de hospedagem. Por exemplo:

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

   $result

   $result.ProvResourceInStorage | Format-List -Property *
   ```

   Após uma migração bem-sucedida, o MCS remove automaticamente o disco base obsoleto e não há máquinas no armazenamento antigo. Portanto, após executar o comando, certifique-se de que não há máquinas e disco base no armazenamento antigo.
2. Execute `Remove-Hyphostingunitstorage` para remover completamente o armazenamento antigo da unidade de hospedagem. Você também pode usar o Web Studio para remover o armazenamento antigo.

### Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "chave":"valor".

| NOME DO RECURSO | TAG |
| --- | --- |
| VM de Preparo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| NOME DO RECURSO | TAG |
|---|---|
| | "XdConfig:"XdProvisioned=True" |
| VM no catálogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| | "XdConfig:"XdProvisioned=True" |

### Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Criar catálogos de máquinas
- Criar um catálogo VMware
- Gerenciar catálogos de máquinas

## Gerenciamento de Energia

Com o Citrix Virtual Apps and Desktops™, você pode gerenciar o consumo de energia de VMs provisionadas por MCS em vários hipervisores e serviços de nuvem suportados. A operação de gerenciamento de energia oferece a você:

- Experiência ideal do usuário
- Gerenciamento de custos e economia de energia

As ações de energia disponíveis são:

- Iniciar
- Desligar
- Reiniciar
- Suspender
- Retomar
- Forçar reinício
- Desligamento forçado

> **Observação:**

- Para uma VM não persistente, o ciclo de energia (desligar/iniciar e reiniciar) resulta na redefinição do disco do SO.
- As capacidades e comportamentos das ações de energia variam dependendo de hipervisores ou serviços de nuvem.

O artigo aborda os principais recursos de gerenciamento de energia associados a certos hipervisores suportados.

- Gerenciar energia de VMs AWS
- Gerenciar energia de VMs Azure

## Gerenciar energia de VMs AWS

Para obter informações sobre as permissões necessárias, consulte Permissões AWS necessárias.

### Hibernação de Instância

O processo de hibernação armazena o estado em memória da instância, juntamente com seus endereços IP privados e elásticos, permitindo que ela retome exatamente de onde parou.

Quando uma instância é instruída a hibernar, ela grava o estado em memória em um arquivo no volume EBS raiz e, em seguida, se desliga. Um volume Amazon EBS é um dispositivo de armazenamento durável, em nível de bloco, que você pode anexar às suas instâncias. Depois de anexar um volume a uma instância, você pode usá-lo como usaria um disco rígido físico. Criptografe o volume EBS raiz da instância. A criptografia garante a proteção adequada para dados confidenciais quando são copiados da memória para o volume EBS. Para obter informações sobre a criptografia EBS, consulte Criptografia Amazon EBS.

A seguir estão as limitações da hibernação de instância suportada:

- Memória da instância (RAM) de apenas até 150 GB é suportada
- O modo de inicialização UEFI não é suportado
- Os SSDs de uso geral e os SSDs de IOPS provisionadas são suportados apenas como tipos de volume EBS.

#### Criar VMs com suporte a hibernação

Para criar VMs com suporte a hibernação:

1. Crie uma conexão de host. Consulte Conexão com a AWS.

2. Inicie uma instância com a raiz EBS criptografada e a propriedade **Stop-Hibernate** ativada. Para obter mais informações sobre como iniciar a instância, criptografar o volume raiz EBS e ativar a hibernação, consulte `<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`. Use esta instância como uma imagem mestre para criar uma AMI.
3. Prepare a imagem mestre:
   a. Instale um VDA na imagem mestre. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe. Para obter mais informações sobre como instalar um VDA, consulte Instalar VDAs.
   b. Una a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas.
4. Crie uma AMI a partir dessa instância. Para obter informações sobre como criar uma AMI a partir de uma instância, consulte Criar uma AMI a partir de uma instância do Amazon EC2.
5. Crie um catálogo de máquinas usando o comando `New-ProvScheme`. Defina a propriedade personalizada `AwsCaptureInstanceProperties` como **True**.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

   Para obter informações sobre como criar um catálogo de máquinas usando comandos PowerShell, consulte `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>`.

As VMs que podem ser hibernadas são criadas se:

- Você selecionar uma AMI criada a partir de uma imagem mestre que tenha a propriedade **Stop-Hibernate** habilitada.
- A VM mestre estiver unida ao domínio e tiver o VDA instalado.
- Você seleciona o tamanho correto da VM (oferta de serviço) que pode manipular a hibernação.

O comando **New-ProvScheme** falha com uma mensagem de erro apropriada se:

- A VM mestre está habilitada para hibernação, mas a oferta de serviço não é capaz de lidar com a hibernação.
- Se a VM mestre não estiver ingressada no domínio e não tiver nenhum VDA instalado.

### Status de hibernação de ofertas de serviço e AMI

Para obter o status de hibernação das ofertas de serviço e AMI (modelos), execute os seguintes comandos:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

### Atualizar oferta de serviço de um esquema de provisionamento existente com suporte a hibernação

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

O sistema exibe uma mensagem de exceção se a oferta de serviço não for compatível.

### Atualizar catálogo de máquinas que suporta hibernação

Se você tentar atualizar um catálogo de máquinas existente com um catálogo de máquinas que não suporta hibernação, a atualização falhará com uma mensagem de erro apropriada.

### Gerenciamento de energia de VMs hibernadas

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs hibernadas:

1. Suspender a VM do estado de execução.
2. Retomar a VM do estado suspenso.
3. Reiniciar a VM do estado suspenso.

## Gerenciar energia de VMs do Azure

Para obter informações sobre as permissões necessárias, consulte Permissões do Azure necessárias.

### Provisionamento sob demanda do Azure

Com o provisionamento sob demanda do Azure, as VMs são criadas apenas quando o Citrix Virtual Apps and Desktops™ inicia uma ação de inicialização, após a conclusão do provisionamento.

Ao usar o MCS para criar catálogos de máquinas no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz seus custos de armazenamento
- Oferece criação de catálogo mais rápida

Ao criar um catálogo MCS, o portal do Azure exibe os grupos de segurança de rede, interfaces de rede, imagens base e discos de identidade nos grupos de recursos.

O portal do Azure não mostra uma VM até que o Citrix Virtual Apps and Desktops inicie uma ação de inicialização para ela. Existem dois tipos de máquinas com as seguintes diferenças:

- Para uma máquina agrupada, o disco do sistema operacional e o cache de write-back existem apenas quando a VM existe. Ao desligar uma máquina agrupada no console, a VM não fica visível no portal do Azure. Há uma economia significativa de custos de armazenamento se você desligar as máquinas rotineiramente (por exemplo, fora do horário de trabalho).
- Para uma máquina dedicada, o disco do sistema operacional é criado na primeira vez que a VM é ligada. A VM no portal do Azure permanece no armazenamento até que a identidade da máquina seja excluída. Ao desligar uma máquina dedicada no console, a VM ainda fica visível no portal do Azure.

> **Nota:**
>
> O suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos “legados”) foi descontinuado. Portanto, recrie as VMs de catálogo

legado do Azure. Os catálogos são então provisionados sob demanda, o que economiza custos de armazenamento.

### Preservar uma máquina virtual provisionada ao reiniciar

Escolha se deseja preservar uma máquina virtual provisionada ao reiniciar. Use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provisionada persiste quando reiniciada. Defina a propriedade `PersistVm` como **true** para manter uma máquina virtual quando desligada, ou defina a propriedade como **false** para garantir que a máquina virtual não seja preservada quando desligada.

**Nota:**

A propriedade `PersistVm` se aplica apenas a um esquema de provisionamento com as propriedades `CleanOnBoot` e `UseWriteBackCache` ativadas. Se a propriedade `PersistVm` não for especificada para máquinas virtuais não persistentes, elas serão excluídas do ambiente Azure quando desligadas.

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` define a propriedade `PersistVm` como **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />
```

```
<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` preserva o cache de write-back definindo `PersistVM` como **true**:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
```

```
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

**Dica:**

A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco do SO deve persistir. Para preservar uma máquina virtual provisionada, preserve o disco do SO primeiro. Não exclua o disco do SO sem antes excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem especificar o parâmetro `PersistVm`.

### Personalizar o comportamento de ligar em caso de falha na alteração do tipo de armazenamento

Ao ligar, o tipo de armazenamento de um disco gerenciado pode falhar ao mudar para o tipo desejado devido a uma falha no Azure. Nesses cenários, a VM permaneceria desligada com uma mensagem de falha enviada a você. No entanto, você pode optar por ligar a VM mesmo quando o armazenamento não puder ser restaurado para o tipo configurado ou optar por manter a VM desligada.

- Se você configurar a propriedade personalizada `FailSafeStorageType` como **true** (configuração padrão) ou não a especificar nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM é iniciada com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.
- Se você configurar a propriedade personalizada `FailSafeStorageType` como **false** nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM permanece desligada com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.

Para criar um catálogo de máquinas:

1. Abra uma janela do PowerShell.

2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado.
4. Adicione a propriedade personalizada em `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. Crie o catálogo de máquinas. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

Para atualizar um catálogo de máquinas existente para incluir a propriedade personalizada `FailSafeStorageType`. Esta atualização não afeta as VMs existentes.

1. Atualize a propriedade personalizada no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Para aplicar a alteração feita em Set-ProvScheme às VMs existentes, execute o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

1. Execute o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`. Por exemplo:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. Reinicie as VMs.

### Criar VMs com capacidade de hibernação

Em ambientes Azure, você pode criar um catálogo de máquinas MCS que suporta hibernação. Usando este recurso, você pode suspender uma VM e, em seguida, reconectar-se ao estado anterior da VM quando um usuário fizer login novamente.

A capacidade de hibernação aplica-se ao seguinte:

- SO de sessão única
- VMs persistentes e não persistentes
- Desktops VDI estáticos e aleatórios (agrupados)

Você pode retomar a mesma sessão depois de hibernar uma VM, independentemente de o desktop VDI ser estático ou aleatório.

Nesta seção, consulte o seguinte:

- Pré-requisitos
- Limitações
- Criar e gerenciar um catálogo de máquinas com capacidade de hibernação
- Criar um catálogo de máquinas para VMs existentes com capacidade de hibernação
- Verificar a propriedade de hibernação
- Gerenciamento de energia de VMs (Manual e Automatizado)

**Pré-requisitos para usar a hibernação**

Para usar a hibernação, certifique-se de concluir as seguintes tarefas:

- Instale o Agente de VM do Azure na imagem mestre para Windows e Linux. O arquivo de paginação da imagem do Windows pode estar no disco temporário. O MCS define o local do arquivo de paginação para a unidade C: no disco base quando a hibernação é ativada no catálogo de máquinas.
- O MCS define automaticamente a propriedade de hibernação para os recursos gerados. Você não precisa configurar as propriedades dos recursos mestre para oferecer suporte à hibernação.
- Use um tamanho de VM em sua assinatura que suporte a hibernação.
- Crie um perfil de máquina com capacidade de hibernação (VM ou especificação de modelo) para que as VMs herdem a capacidade de hibernação. Para criar a VM, consulte Introdução à hibernação.

> **Nota:**
>
> De acordo com a Microsoft, você pode implantar VMs com hibernação ativada a partir de um disco de SO. Este recurso é atualmente suportado em certas regiões e estará disponível para todas as regiões em breve. Para mais informações, consulte Implantar VMs com hibernação ativada a partir de um disco de SO.

> Para criar a especificação do modelo, faça o seguinte:

a. Abra o Portal do Azure. Escolha uma VM cuja configuração você deseja usar no modelo. Selecione **Exportar modelo** no painel esquerdo.

b. Desmarque a caixa de seleção **Incluir parâmetros**. Copie o contexto e salve-o como um arquivo JSON, por exemplo, `VMExportTemplate.json`.

c. Certifique-se de que o parâmetro `hibernationEnabled` esteja `true` no modelo. Se o parâmetro não estiver `true`, verifique a configuração da VM que você usou. Você pode especificar um tamanho de VM suportado no arquivo de modelo. No entanto, você também pode especificar o tamanho da máquina ao criar o catálogo.

d. Adicione o modelo para o recurso de interface de rede ao arquivo JSON `VMExportTemplate.json`. Como resultado, você terá um arquivo de modelo ARM com dois recursos.

e. Selecione **Portal do Azure > Especificações de modelo > Importar modelo > Escolher arquivo de modelo local** para importar este arquivo de modelo como uma especificação de modelo ARM.

f. Após a criação da especificação do modelo ARM, você pode usá-la como um perfil de máquina.

> **Nota:**
>
> Pode levar alguns minutos para sincronizar com o Citrix Studio.

Para mais informações, consulte o documento da Microsoft Pré-requisitos para usar a hibernação.

**Limitações**

- Apenas catálogos de máquinas de SO de sessão única (persistentes e não persistentes) são suportados.
- Discos de SO efêmeros e recursos de E/S do MCS não suportam a hibernação do Azure.
- A hibernação pode falhar durante as atualizações automáticas do Windows.

Para obter mais informações, consulte o documento da Microsoft.

**Criar e gerenciar um catálogo de máquinas com capacidade de hibernação**

Para criar VMs com capacidade de hibernação, você pode criar e gerenciar um catálogo de máquinas com capacidade de hibernação usando:

- Web Studio, ou

- Comandos do PowerShell

### CRIAR UM CATÁLOGO USANDO O WEB STUDIO

1. Selecione **Criar Catálogo de Máquinas**. O assistente de criação de catálogo será aberto.
2. Na página **Tipo de Máquina**, selecione o tipo de máquina **SO de sessão única** para este catálogo.
3. Na página **Gerenciamento de Máquinas**, selecione as configurações da seguinte forma:
    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
    b. Selecione **Citrix Machine Creation Services™ (MCS)**.
4. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho aleatória ou estática conforme necessário.
5. Na página **Imagem**, selecione uma imagem mestre. Marque a caixa de seleção **Usar um perfil de máquina** e selecione um perfil de máquina que suporte hibernação. Clique na dica de ferramenta para saber se um perfil de máquina suporta hibernação.
6. Na página **Tipos de Armazenamento e Licença**, selecione o armazenamento e a licença a serem usados para este catálogo.
7. Na página **Máquinas Virtuais**, selecione a contagem de VMs, o tamanho da VM e a zona de disponibilidade.

> **Observação:**
>
> Os tamanhos de máquina que suportam hibernação são mostrados apenas para sua seleção.

8. Na página **NICs**, adicione as NICs que você deseja que as VMs usem.
9. Na página **Configurações de Disco**, selecione o tipo de armazenamento e o tamanho do disco de cache de write-back.
10. Na página **Grupo de Recursos**, selecione o grupo de recursos para provisionar VMs.
11. Na página **Identidades da Máquina**, selecione **Criar novas contas do Active Directory**. Em seguida, especifique um esquema de nomenclatura de conta.
12. Na página **Credenciais de Domínio**, clique em **Inserir credenciais**. Insira suas credenciais de domínio para realizar a criação da conta no domínio do Active Directory de destino.

13. Na página **Resumo**, insira um nome para o catálogo de máquinas e clique em **Concluir**.

Quando a criação do catálogo de máquinas MCS estiver concluída, localize o catálogo na lista de catálogos e clique na guia **Propriedades do Modelo**. O valor do parâmetro **Hibernação** deve ser **Suportado**.

Se você deseja editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar.
  - Alterar o perfil da máquina para um que não seja capaz de hibernar.
- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
  - atualmente, altere o perfil da máquina para um capaz de hibernar usando o Web Studio.

### CRIAR UM CATÁLOGO DE MÁQUINAS PARA GERENCIAR VMS EXISTENTES CAPAZES DE HIBERNAR

Se você já tiver VMs capazes de hibernar e quiser suspendê-las e retomá-las, crie um catálogo de máquinas para importar essas VMs para gerenciamento de energia.

> **Nota:**

> Você pode criar um catálogo de máquinas contendo VMs capazes e incapazes de hibernar. No entanto, se você quiser funcionalidade relacionada à hibernação, você deve criar o catálogo de máquinas apenas com VMs capazes de hibernar.

> Para criar um catálogo para VMs existentes capazes de hibernar usando o Web Studio, siga as instruções na tela para concluir as etapas e preste atenção às seguintes configurações principais:

1. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e, em seguida, selecione **Outro serviço ou tecnologia** como a forma de implantar máquinas.
2. Na página **Máquinas Virtuais**, adicione ou importe apenas as VMs capazes de hibernar.

### CRIAR UM CATÁLOGO DE MÁQUINAS USANDO COMANDOS DO POWERSHELL

Depois de atender a todos os requisitos para usar a hibernação, você pode criar um catálogo de máquinas capaz de hibernar usando o comando `New-ProvScheme`. Para obter informações sobre como criar um catálogo usando o SDK do Remote PowerShell, consulte New-ProvScheme.

Ao criar o catálogo, você pode verificar se um tamanho de VM e um perfil de máquina suportam hibernação ou não usando os seguintes comandos do PowerShell:

- Para o tamanho da VM, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- Para o perfil da máquina, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

Se você deseja editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar
  - Alterar o perfil da máquina para um que não seja capaz de hibernar
- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
  - atualmente, altere o perfil da máquina para um capaz de hibernar usando o Web Studio.

Para obter informações sobre como modificar o tamanho da VM e o perfil da máquina de um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

### Verificar propriedade de hibernação

Você pode verificar a propriedade de hibernação de um catálogo de máquinas, VM e uma máquina broker usando os comandos do PowerShell:

- Para verificar a propriedade de hibernação de um esquema de provisionamento, execute os seguintes comandos do PowerShell. O parâmetro `HibernationEnabled` deve ser `True`.

  ```
  (Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
  -join "" |  ConvertFrom-Json | Select HibernationEnabled
  ```

- Para verificar a propriedade de hibernação de uma VM de provisionamento, execute os seguintes comandos do PowerShell. O parâmetro `SupportsHibernation` deve ser `True`.

  ```
  (Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
  Select SupportsHibernation
  ```

- Para verificar a capacidade de hibernação de uma máquina broker, execute os seguintes comandos PowerShell. As ações de energia **Suspender** e **Retomar** indicam capacidade de hibernação.

  ```
  (Get-BrokerMachine -MachineName
  <YourMachineName>).SupportedPowerActions
  ```

### Gerenciamento de energia de VMs capazes de hibernar

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs com capacidade de hibernação:

- **Suspender** VM do estado de execução
- **Retomar** VM do estado suspenso
- **Forçar desligamento** da VM de um estado suspenso
- **Forçar reinício** da VM do estado suspenso

Consulte o seguinte para obter mais informações:

- Suspender
- Retomar

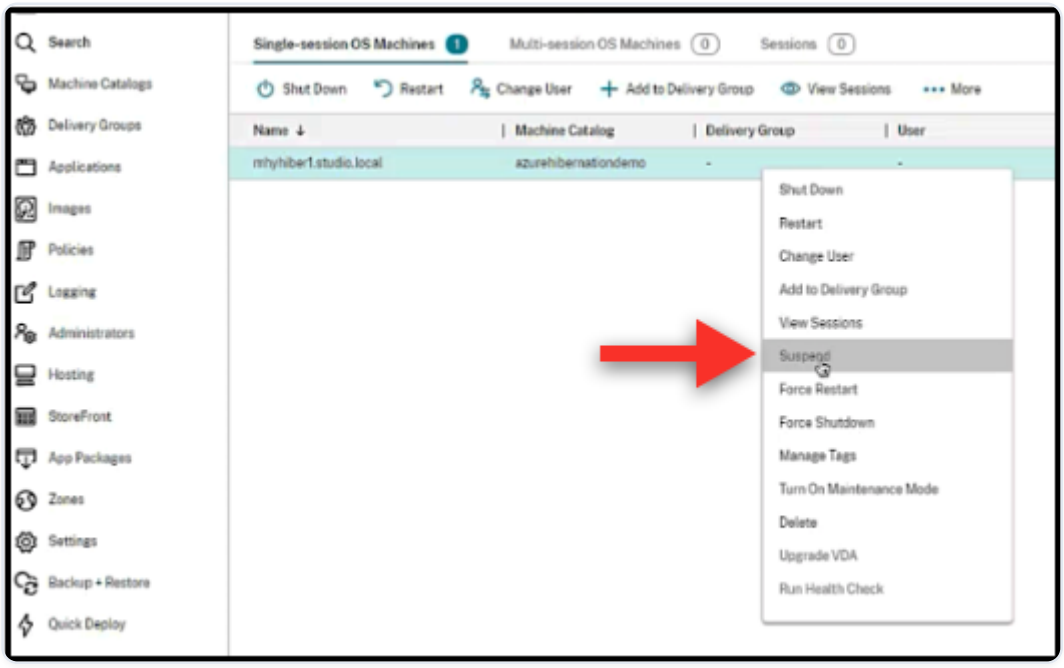
### SUSPENDER

Você pode suspender uma VM usando uma das seguintes maneiras:

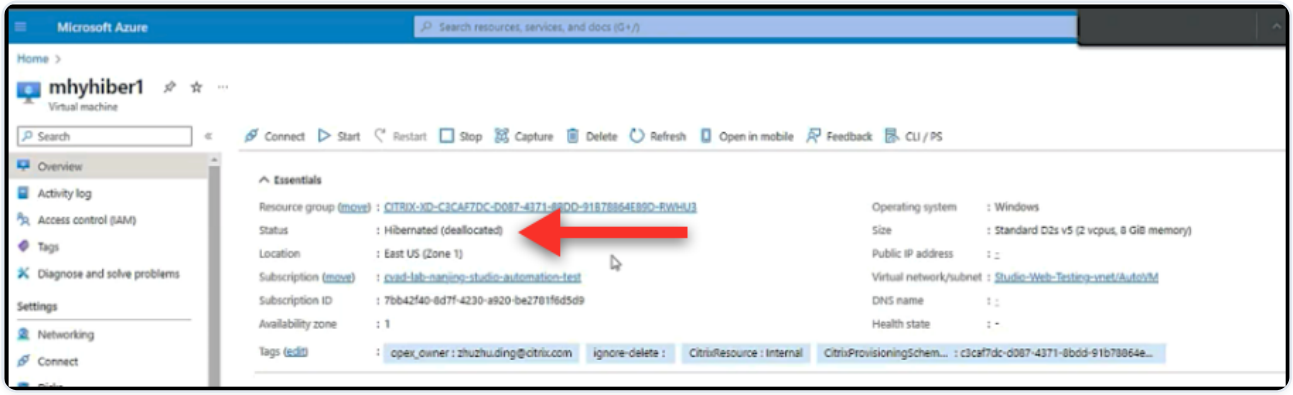
- **Manualmente** usando o Web Studio
- **Automaticamente** usando a política de tempo limite: Para obter mais informações, consulte Configurações diversas.

Para suspender manualmente uma VM:

1. Clique com o botão direito na VM e selecione **Suspender**. Clique em **Sim** para confirmar a ação. O **Estado de Energia** muda de **Suspensão** para **Suspenso**.




Você pode verificar o status da VM no portal do Azure.

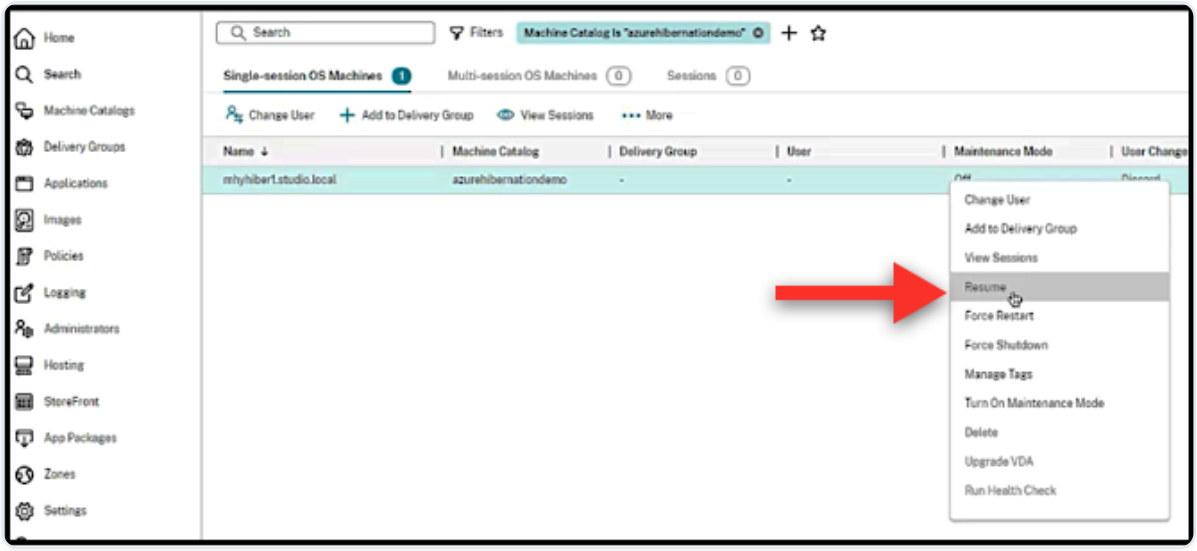



### RETOMAR

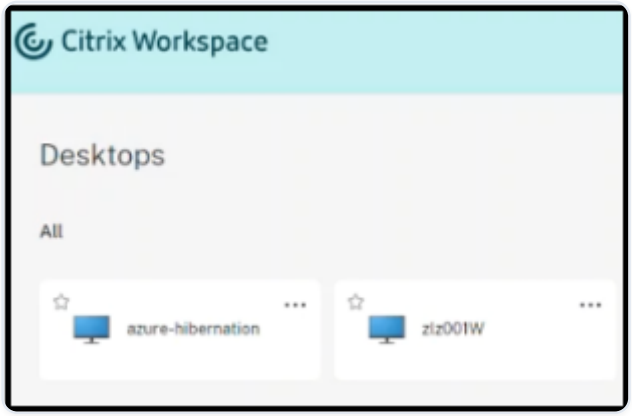
Para retomar uma VM hibernada, use uma das seguintes maneiras:

- **Manualmente**:

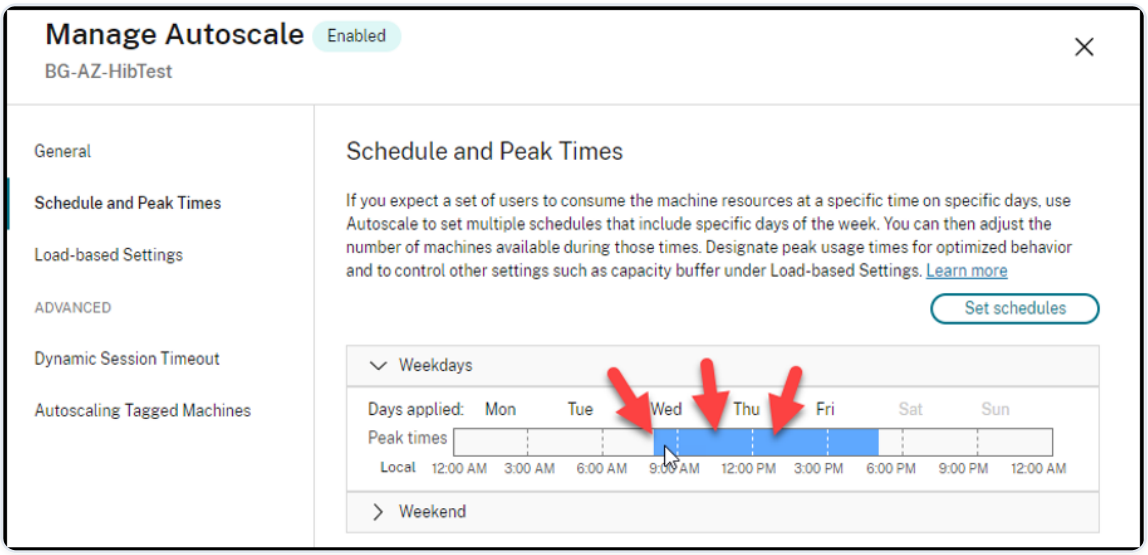
- Os administradores podem retomar a VM usando o Web Studio.



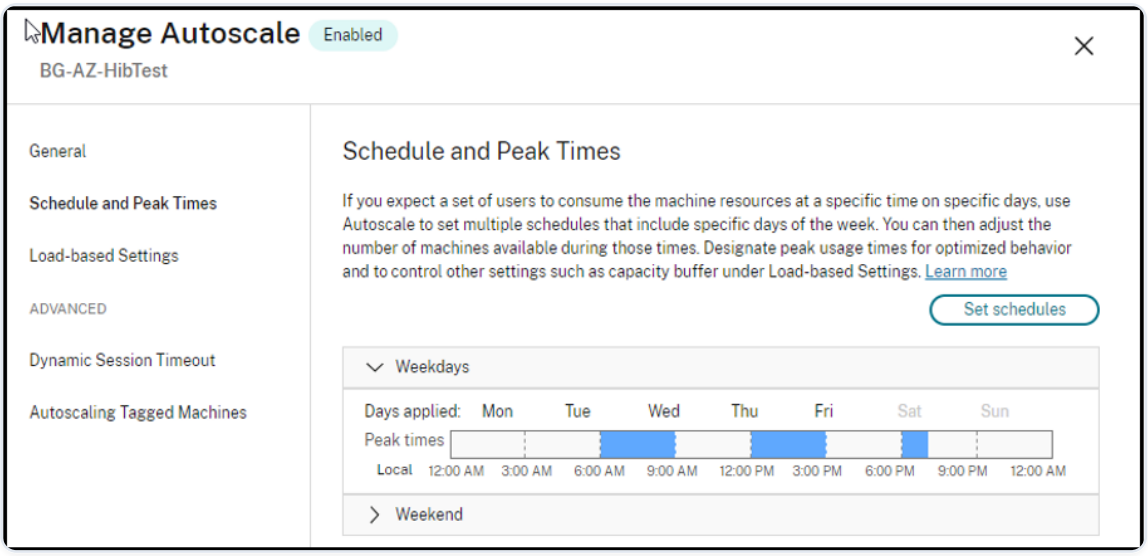

- Os usuários finais podem iniciar a VM usando o menu do Citrix Workspace™ assim que clicarem no ícone da área de trabalho.




- **Automaticamente**:
  - O Autoscale™ pode ligar automaticamente as máquinas hibernadas se você configurar os horários de pico corretamente. Você pode definir os horários de pico em intervalos de 30 minutos clicando na programação de horários. Cada quadro azul representa um slot de tempo marcado como horário de pico. Os horários de pico podem ter slots de tempo consecutivos e não consecutivos.
    - Slots de tempo consecutivos

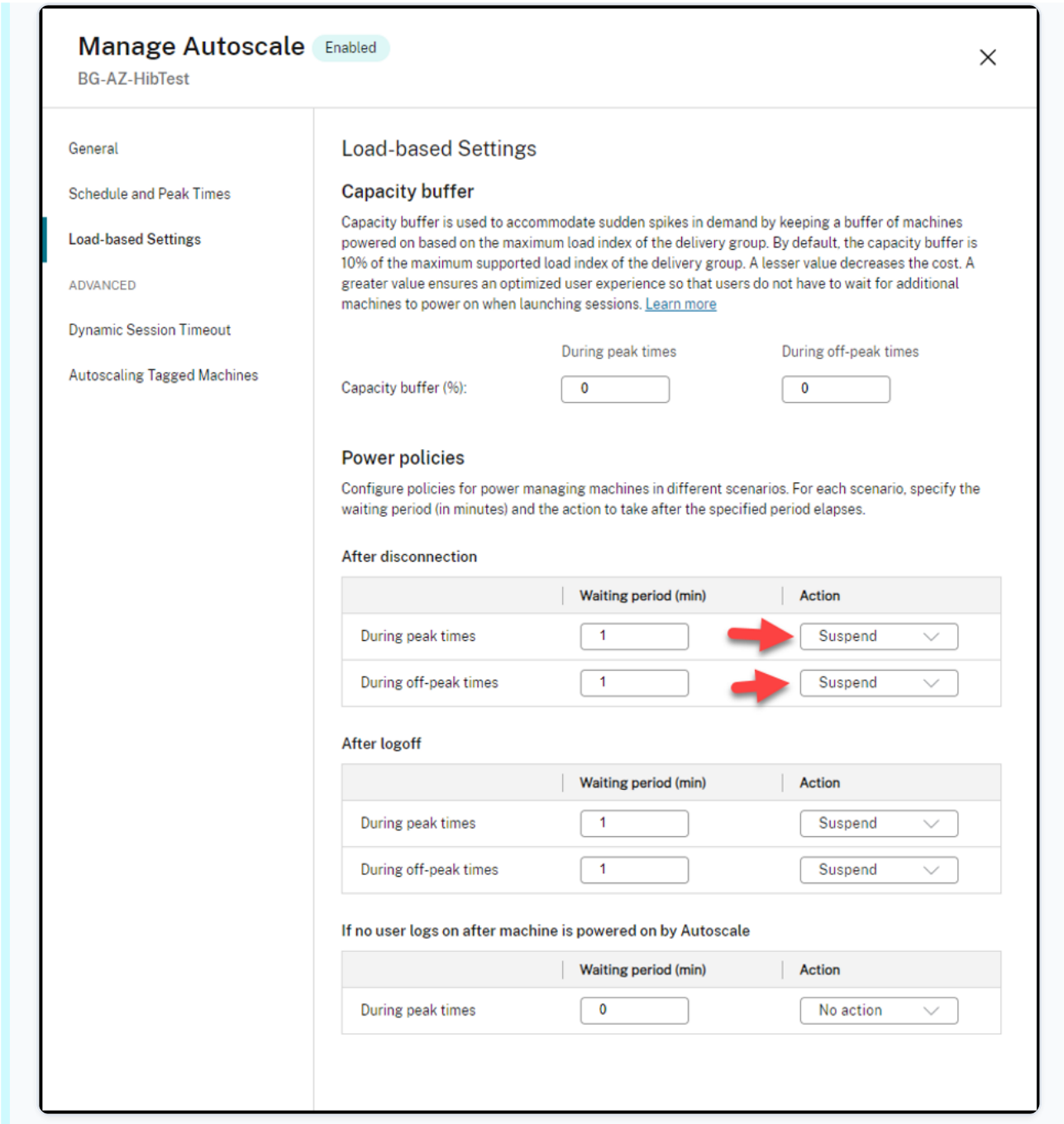



- Slots de tempo não consecutivos




**Nota:**

Em **Gerenciar Autoescala > Configurações baseadas em carga**, se a **Ação** estiver configurada como **Suspender**, então certifique-se de que todas as VMs dentro desse grupo de entrega tenham capacidade de hibernação. Caso contrário, as VMs que não podem hibernar continuarão a ser executadas.




### Mais informações

Para obter mais informações sobre a hibernação do Citrix Azure, consulte o artigo da Citrix Tech Zone.

# Políticas de segurança

## Grupos de segurança

O grupo de segurança é um grupo de regras de segurança para filtrar o tráfego de rede entre recursos em uma rede virtual. As regras de segurança permitem ou negam o tráfego de rede de

entrada para, ou o tráfego de rede de saída de, vários tipos de recursos. Cada regra especifica as seguintes propriedades:

- Nome: Um nome exclusivo dentro do grupo de segurança de rede
- Prioridade: As regras são processadas em ordem de prioridade, com números menores processados antes de números maiores, porque números menores têm prioridade mais alta
- Origem ou Destino: Qualquer, ou um endereço IP individual, bloco de roteamento entre domínios sem classe (CIDR) (10.0.0.0/24, por exemplo), tag de serviço ou grupo de segurança de aplicativo
- Protocolo: Os protocolos com base nos quais você adiciona regras para cada grupo de segurança
- Direção: Se a regra se aplica ao tráfego de entrada ou de saída
- Intervalo de portas: Você pode especificar uma porta individual ou um intervalo de portas
- Ação: Permitir ou negar

Consulte o seguinte para obter mais informações sobre hipervisores suportados:

- Grupos de segurança na AWS
- Grupos de segurança no Microsoft Azure
- Grupos de segurança no Google Cloud Platform

### Grupos de segurança na AWS

Os grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também pode associar esses grupos de segurança a cada instância em sua VPC. As regras de entrada controlam o tráfego de entrada para sua instância, e as regras de saída controlam o tráfego de saída de sua instância.

Para obter mais informações sobre a configuração de rede durante a preparação da imagem, consulte Configuração de rede durante a preparação da imagem.

Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança. Para configurar grupos de segurança, consulte Configurar grupos de segurança.

### Grupos de segurança no Microsoft Azure

O Citrix Virtual Apps and Desktops oferece suporte a grupos de segurança de rede no Azure. Espera-se que os grupos de segurança de rede se associem a sub-redes. Para obter mais informações, consulte Grupos de segurança de rede.

Para obter mais informações sobre o grupo de segurança de rede criado durante a preparação da imagem, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

### Grupos de segurança no Google Cloud Platform

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como disco do sistema da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total. Para obter mais informações, consulte Regras de Firewall.

## Inicialização Segura e vTPM

A Inicialização Segura é um recurso da Unified Extensible Firmware Interface (UEFI), que é responsável pela inicialização do sistema. Ela garante que apenas software confiável seja carregado durante o processo de inicialização.

Módulo de Plataforma Confiável (TPM) é um chip de hardware que fornece armazenamento seguro para chaves criptográficas e outros dados confidenciais. Um Módulo de Plataforma Confiável Virtual (vTPM) executa as mesmas funções que um TPM, mas executa recursos de coprocessador criptográfico em software. Embora o TPM possa aumentar a segurança, não é um requisito para o Secure Boot.

Consulte o seguinte para obter mais informações sobre os serviços de nuvem suportados:

- Inicialização Segura e vTPM no Google Cloud Platform
- Inicialização Segura e vTPM no Microsoft Azure
- vTPM no VMware

### Inicialização Segura e vTPM no Google Cloud Platform

Você pode provisionar máquinas virtuais blindadas no Google Cloud Platform (GCP). A integridade verificável da VM blindada é alcançada usando os seguintes recursos:

- Inicialização Segura
- Inicialização Medida habilitada para vTPM
- Monitoramento de integridade

Para obter mais informações sobre como usar o PowerShell para criar um catálogo com VM blindada, consulte Usando o PowerShell para criar um catálogo com VM blindada.

> **Nota:**
>
> Se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, se você usar um perfil de máquina para criar o catálogo, deverá habilitar o vTPM na origem do perfil de máquina (VM ou modelo de instância). Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte Criar VMs do Windows 11 no nó de locatário único.

### Inicialização Segura e vTPM no Microsoft Azure

Em ambientes Azure, você pode criar catálogos de máquinas habilitados com o Trusted Launch. O Azure oferece o Trusted Launch como uma forma contínua de melhorar a segurança das VMs de geração 2. O Trusted Launch protege contra técnicas de ataque avançadas e persistentes. Para habilitar o Trusted Launch, use uma configuração de catálogo baseada em perfil de máquina. Na raiz do Trusted Launch está o Secure Boot para sua VM. O Trusted Launch também usa o vTPM para realizar atestado remoto pela nuvem. Isso é usado para verificações de integridade da plataforma e para tomar decisões baseadas em confiança. Você pode habilitar individualmente o Secure Boot e o vTPM. Para obter mais informações sobre como criar um catálogo de máquinas com o Trusted Launch, consulte Catálogos de máquinas com Trusted Launch.

### vTPM no VMware

O MCS oferece suporte à criação de um catálogo de máquinas com vTPM. Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Se a configuração baseada em perfil de máquina for usada e o vTPM estiver habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM do modelo de VM. Se o perfil de máquina não for usado e a imagem mestre tiver o vTPM habilitado, as VMs no catálogo terão o vTPM em branco. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

# Recursos de criptografia

Os recursos de criptografia protegem o conteúdo das máquinas virtuais contra ataques de convidados mal-intencionados em um host de máquina virtual compartilhado e contra ataques lançados pelo software de controle do hipervisor que gerencia todas as máquinas virtuais no host.

Consulte o seguinte para obter mais informações sobre os serviços de nuvem compatíveis:

- Recursos de criptografia na AWS
- Recursos de criptografia no Google Cloud Platform
- Recursos de criptografia no Microsoft Azure

## Recursos de criptografia na AWS

Esta seção descreve os recursos de criptografia em ambientes de virtualização da AWS.

### Criptografia automática

Você pode ativar a criptografia automática de novos volumes Amazon EBS e cópias de snapshot criadas em sua conta. Para obter mais informações, consulte Criptografia automática.

## Recursos de criptografia no Google Cloud Platform

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Google Cloud Platform (GCP).

Se você precisar de mais controle sobre as operações de chave do que o permitido pelas chaves de criptografia gerenciadas pelo Google, poderá usar chaves de criptografia gerenciadas pelo cliente. Ao usar uma chave de criptografia gerenciada pelo cliente, um objeto é criptografado com a chave pelo Cloud Storage no momento em que é armazenado em um bucket, e o objeto é automaticamente descriptografado pelo Cloud Storage quando é entregue aos solicitantes. Para obter mais informações, consulte Chaves de criptografia gerenciadas pelo cliente.

Você pode usar Chaves de Criptografia Gerenciadas pelo Cliente (CMEK) para catálogos MCS. Para obter mais informações, consulte Usando Chaves de Criptografia Gerenciadas pelo Cliente (CMEK).

## Recursos de criptografia no Microsoft Azure

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Azure.

### Criptografia do lado do servidor do Azure

A maioria dos discos gerenciados do Azure é criptografada com a criptografia do Armazenamento do Azure, que usa criptografia do lado do servidor (SSE) para proteger seus dados e ajudar você a

cumprir seus compromissos de segurança e conformidade. O Citrix Virtual Apps and Desktops oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

### Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host.

Este método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, este método de criptografia criptografa os dados de ponta a ponta.

Para obter mais informações sobre como criar um catálogo de máquinas MCS com capacidade de criptografia no host, consulte Criptografia de disco do Azure no host.

### Criptografia dupla do Azure

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente com alta sensibilidade à segurança e preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por esta criptografia dupla. Discos de SO e de dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla em disco gerenciado.

### VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto a VM quanto o modelo ARM como entrada de perfil de máquina.

Para obter mais informações, consulte VMs confidenciais do Azure.

## Criar grupos de entrega

> **Nota:**

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

> Um grupo de entrega é uma coleção de máquinas selecionadas de um ou mais catálogos de máquinas. O grupo de entrega especifica quais usuários podem usar essas máquinas, além dos aplicativos e desktops disponíveis para esses usuários.

Criar um grupo de entrega é o próximo passo na configuração da sua implantação após criar um site e criar um catálogo de máquinas. Posteriormente, você pode alterar as configurações iniciais no primeiro grupo de entrega e criar outros grupos de entrega. Existem também recursos e configurações que você pode configurar apenas ao editar um grupo de entrega, e não ao criá-lo.

**Nota:**

> O Autoscale™ é habilitado por padrão se você criar ou atualizar Grupos de Entrega usando o Studio baseado em MMC.

> Para Acesso Remoto a PC, ao criar um site, um grupo de entrega chamado "Remote PC Access Desktops" é criado automaticamente.

Para criar um grupo de entrega:

1. Se você criou um site e um catálogo de máquinas sem um grupo de entrega, o Web Studio o guiará para o local de início correto para criar um.
2. Se você já criou um grupo de entrega e deseja criar outro, siga estas etapas:
    a. Selecione **Grupos de Entrega**. Selecione **Criar Grupo de Entrega** no painel de ações.
    b. Para organizar grupos de entrega usando pastas, crie pastas sob a pasta padrão **Grupos de Entrega**. Para obter mais informações, consulte Criar uma pasta.
    c. Selecione a pasta onde você deseja criar o grupo e, em seguida, clique em **Criar Grupo de Entrega**. O assistente de criação de grupo é aberto.
3. O assistente é iniciado com uma página de **Introdução**, que você pode remover de futuras inicializações deste assistente.

4. O assistente o guiará pelas páginas descritas na seção a seguir. Ao terminar cada página, clique em **Avançar** até chegar à página final.

## Etapa 1. Máquinas

Na página **Máquinas**, selecione um catálogo e selecione o número de máquinas que você deseja usar desse catálogo.

É bom saber:

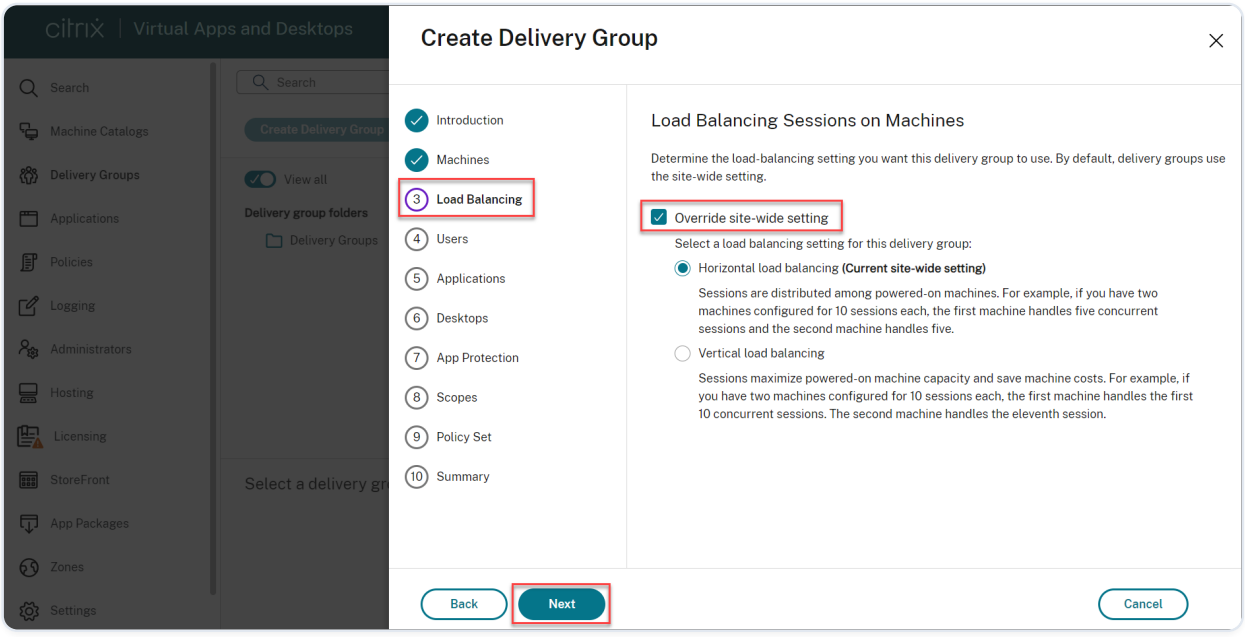
- Pelo menos uma máquina deve permanecer sem uso em um catálogo selecionado.
- Um catálogo pode ser especificado em mais de um grupo de entrega. Uma máquina pode ser usada em apenas um grupo de entrega.
- Um grupo de entrega pode usar máquinas de mais de um catálogo; no entanto, esses catálogos devem conter os mesmos tipos de máquina (SO multi-sessão, SO de sessão única ou Acesso Remoto a PC). Em outras palavras, você não pode misturar tipos de máquina em um grupo de entrega. Da mesma forma, se sua implantação tiver catálogos de máquinas Windows e catálogos de máquinas Linux, um grupo de entrega pode conter máquinas de qualquer um dos tipos de SO, mas não de ambos.
- A Citrix recomenda que você instale ou atualize todas as máquinas com a versão mais recente do VDA. Atualize catálogos e grupos de entrega conforme necessário. Ao criar um grupo de entrega, se você selecionar máquinas que têm diferentes versões de VDA instaladas, o grupo de entrega será compatível com a versão mais antiga do VDA. Isso é chamado de *nível funcional* do grupo. Por exemplo, se uma das máquinas tiver a versão 7.1 do VDA e as outras máquinas tiverem a versão atual, todas as máquinas no grupo poderão usar apenas os recursos que foram suportados no VDA 7.1. Isso significa que alguns recursos que exigem versões posteriores do VDA podem não estar disponíveis nesse grupo de entrega.
- Cada máquina em um catálogo de Acesso Remoto a PC é automaticamente associada a um grupo de entrega. Ao criar um site de Acesso Remoto a PC, um catálogo chamado "Máquinas de Acesso Remoto a PC" e um grupo de entrega chamado "Desktops de Acesso Remoto a PC" são criados automaticamente.
- As seguintes verificações de compatibilidade são realizadas:
  - MinimumFunctionalLevel deve ser compatível
  - SessionSupport deve ser compatível
  - AllocationType deve ser compatível para SingleSession
  - ProvisioningType deve ser compatível

- PersistChanges deve ser compatível para MCS e Citrix Provisioning™
- O catálogo RemotePC é compatível apenas com o catálogo de Acesso Remoto a PC
- Verificação relacionada ao AppDisk

## Etapa 2. Balanceamento de carga

Para configurar as definições de balanceamento de carga ao criar um grupo de entrega:

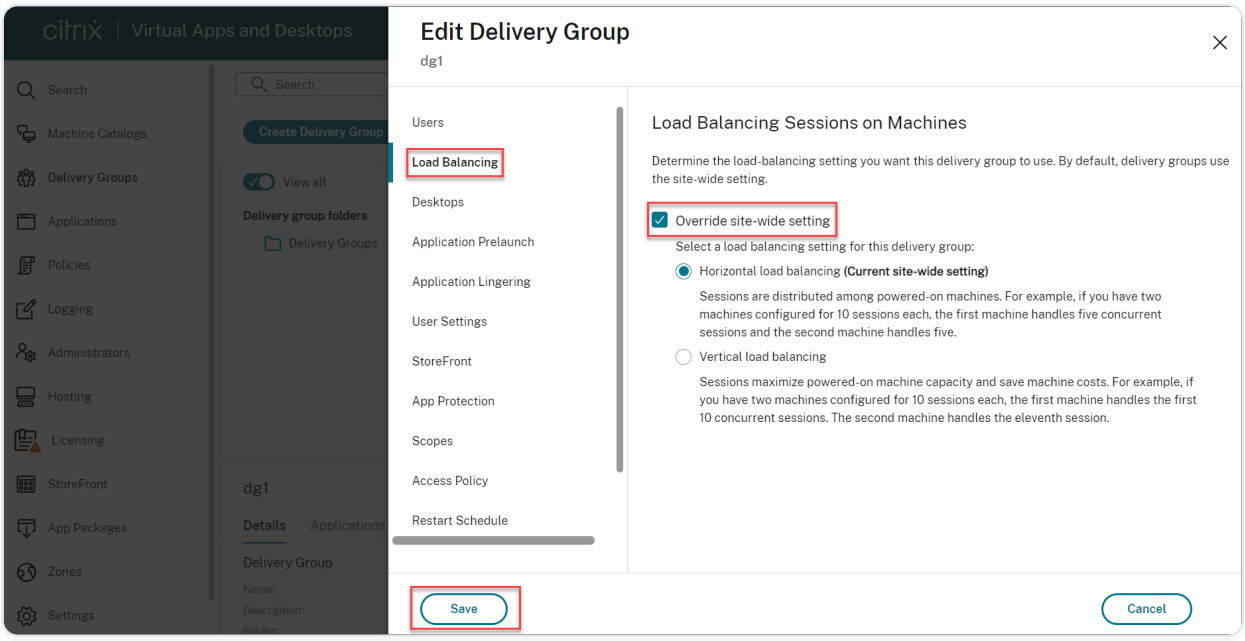
1. Faça login no Web Studio.
2. Na navegação à esquerda, clique em **Grupos de Entrega**.
3. Na página **Grupos de Entrega**, clique em **Criar Grupo de Entrega**.
4. No assistente **Criar Grupo de Entrega**, clique em **Avançar**. O assistente **Máquina** é aberto.
5. No assistente **Máquinas**, selecione um catálogo de máquinas necessário e clique em **Avançar**. O assistente **Balanceamento de Carga** é aberto.
6. No assistente de **Balanceamento de Carga**, selecione a caixa de seleção **Substituir configuração de todo o site**.
7. Selecione a opção **Balanceamento de carga horizontal** ou **Balanceamento de carga vertical** conforme necessário e clique em **Avançar**.




Para configurar as configurações de balanceamento de carga ao editar um grupo de entrega existente:

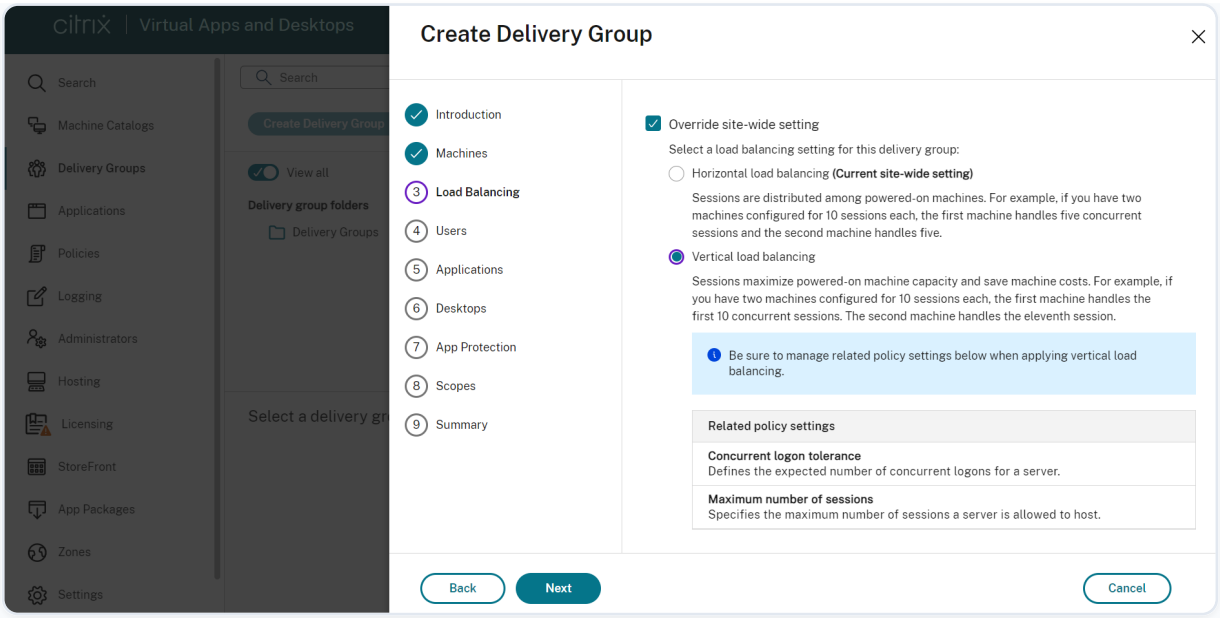
1. Faça login no Web Studio.
2. No painel esquerdo, clique em **Grupos de Entrega**.

3. Selecione um **Grupo de Entrega** na lista e clique em **Editar**. O assistente **Editar Grupo de Entrega** é aberto.
4. Na página **Editar Grupo de Entrega**, clique em **Balanceamento de Carga**.
5. Selecione a caixa de seleção **Substituir configuração de todo o site**.
6. Selecione a opção **Balanceamento de carga horizontal** ou **Balanceamento de carga vertical** conforme necessário e clique em **Salvar**.




**Nota:**

Quando a configuração de balanceamento de carga vertical é aplicada, certifique-se de que as políticas de **Tolerância de logon simultâneo** e **Número máximo de sessões** estejam configuradas adequadamente.




> Para obter mais informações sobre balanceamento de carga no nível do site e do grupo de entrega, consulte Balancear máquinas de carga

## Etapa 3. Tipo de entrega

Esta página aparece somente se você escolheu um catálogo contendo máquinas de SO de sessão única estáticas (atribuídas).

Na página **Tipo de Entrega**, escolha **Aplicativos** ou **Desktops**. Você não pode habilitar ambos.

Se você selecionou máquinas de um catálogo de SO de várias sessões ou de SO de sessão única aleatório (agrupado), o tipo de entrega é considerado aplicativos e desktops: você pode entregar aplicativos, desktops ou ambos.

## Etapa 4. Usuários

Especifique os usuários e grupos de usuários que podem usar os aplicativos e desktops no grupo de entrega.

### Onde as listas de usuários são especificadas

As listas de usuários do Active Directory são especificadas ao criar ou editar o seguinte:

- Uma lista de acesso de usuário de um site, que não é configurada através do Web Studio. Por padrão, as regras da política de direitos de aplicativo incluem todos. Consulte os cmdlets do SDK do PowerShell `BrokerAppEntitlementPolicyRule` para obter detalhes.
- Grupos de aplicativos (se configurados).

- Grupos de entrega.
- Aplicativos.

A lista de usuários que podem acessar um aplicativo através do StoreFront™ é formada pela interseção das listas de usuários acima. Por exemplo, para configurar o uso do aplicativo A para um departamento específico, sem restringir indevidamente o acesso a outros grupos:

- Use a regra de política de direitos de aplicativo padrão que inclui todos.
- Configure a lista de usuários do grupo de entrega para permitir que todos os usuários da sede usem qualquer um dos aplicativos especificados no grupo de entrega.
- (Se os grupos de aplicativos estiverem configurados) Configure a lista de usuários do grupo de aplicativos para permitir que os membros da unidade de negócios de Administração e Finanças acessem os aplicativos A a L.
- Configure as propriedades do aplicativo A para restringir sua visibilidade apenas à equipe de Contas a Receber em Administração e Finanças.

### Usuários autenticados e não autenticados

Existem dois tipos de usuários: autenticados e não autenticados (não autenticados também são chamados de anônimos). Você pode configurar um ou ambos os tipos em um grupo de entrega.

- **Autenticados:** Para acessar aplicativos e desktops, os usuários e membros do grupo que você especificar pelo nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha para o StoreFront ou o aplicativo Citrix Workspace™. Para grupos de entrega que contêm máquinas de SO de sessão única, você pode importar dados de usuário (uma lista de usuários) posteriormente, editando o grupo de entrega.
- **Não autenticados (anônimos):** Para grupos de entrega que contêm máquinas de SO de múltiplas sessões, você pode permitir que os usuários acessem aplicativos e desktops sem apresentar credenciais ao StoreFront ou ao aplicativo Citrix Workspace. Por exemplo, em quiosques, o aplicativo pode exigir credenciais, mas o portal de acesso e as ferramentas Citrix não. Um Grupo de Usuários Anônimos é criado quando você instala o primeiro Delivery Controller.

  Para conceder acesso a usuários não autenticados, cada máquina no grupo de entrega deve ter um VDA para Windows Server OS (versão mínima 7.6) instalado. Quando usuários não autenticados são habilitados, você deve ter uma loja StoreFront não autenticada.

  Contas de usuário não autenticadas são criadas sob demanda quando uma sessão é iniciada e são nomeadas Anon*XYZ*, onde *XYZ* é um valor único de três dígitos.

Sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desconectadas automaticamente quando o cliente se desconecta. Reconexão, roaming entre clientes e Workspace Control não são suportados.

A tabela a seguir descreve suas escolhas na página **Usuários**:

| HABILITAR ACESSO PARA | ADICIONAR/ATRIBUIR USUÁRIOS E GRUPOS DE USUÁRIOS? | HABILITAR A CAIXA DE SELEÇÃO "CONCEDER ACESSO A USUÁRIOS NÃO AUTENTICADOS"? |
|---|---|---|
| Apenas usuários autenticados | Sim | Não |
| Apenas usuários não autenticados | Não | Sim |
| Usuários autenticados e não autenticados | Sim | Sim |

## Etapa 5. Aplicativos

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega de Acesso Remoto para PC.
- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada Aplicativos. Você pode especificar uma pasta diferente. Para obter detalhes, consulte o artigo Gerenciar Aplicativos.
- Você pode alterar as propriedades de um aplicativo ao adicioná-lo a um grupo de entrega, ou posteriormente. Para obter detalhes, consulte o artigo Gerenciar Aplicativos.
- Se você tentar adicionar um aplicativo e já existir um com o mesmo nome nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você recusar, o aplicativo será adicionado com um sufixo que o torna exclusivo dentro dessa pasta de aplicativo.
- Ao adicionar um aplicativo a mais de um grupo de entrega, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos de entrega. Nesses casos, consulte um administrador com permissões maiores ou solicite que seu escopo seja estendido para incluir todos os grupos de entrega aos quais o aplicativo foi adicionado.

- Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade Nome do aplicativo (para usuário) no Web Studio; caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

Clique em **Adicionar** para exibir as fontes do aplicativo.

- **No menu Iniciar:** Aplicativos que são descobertos em uma máquina criada a partir da imagem mestre no catálogo selecionado. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos; selecione os que deseja adicionar e clique em **OK**.
- **Manualmente:** Aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. A seleção desta origem abre uma nova página onde você especifica um aplicativo para adicionar das seguintes maneiras:
  - Digite o caminho para o executável, diretório de trabalho, argumentos opcionais da linha de comando e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Procurar**, insira as credenciais para acessar o VDA, aguarde a conexão com o VDA e, em seguida, selecione um aplicativo do VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.
- **Existente:** Aplicativos adicionados anteriormente ao site, talvez em outro grupo de entrega. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos. Adicione os aplicativos e clique em **OK**.
- **App-V:** Aplicativos em pacotes App-V. Ao selecionar esta origem, uma nova página é aberta onde você seleciona o servidor App-V ou a Biblioteca de Aplicativos. Selecione os aplicativos que deseja adicionar na exibição resultante e clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V.

Se uma origem de aplicativo ou aplicativo não estiver disponível ou for inválido, ele não estará visível ou não poderá ser selecionado. Por exemplo, a origem **Existente** não estará disponível se nenhum aplicativo tiver sido adicionado ao site. Ou, um aplicativo pode não ser compatível com os tipos de sessão suportados em máquinas no catálogo selecionado.

## Etapa 6. Desktops

O título desta página depende do catálogo que você escolheu na página **Máquinas**:

- Se você escolheu um catálogo contendo máquinas agrupadas, esta página é intitulada **Desktops**.

- Se você escolheu um catálogo contendo máquinas atribuídas e especificou "Desktops" na página **Tipo de Entrega**, esta página é intitulada **Atribuições de Usuário de Desktop**.
- Se você escolheu um catálogo contendo máquinas atribuídas e especificou "Aplicativos" na página **Tipo de Entrega**, esta página é intitulada **Atribuições de Usuário de Máquina de Aplicativo**.

Clique em **Adicionar**. Na caixa de diálogo:

- Nos campos Nome de exibição e Descrição, digite as informações a serem exibidas no Citrix Workspace app.
- Para adicionar uma restrição de tag a um desktop, selecione **Restringir inicializações a máquinas com esta tag** e, em seguida, selecione a tag na lista suspensa. Para obter mais informações, consulte Tags.
- Use os botões de rádio para iniciar um desktop ou para atribuir uma máquina ao iniciar o desktop. Os usuários podem ser todos que podem acessar este grupo de entrega, ou usuários e grupos de usuários específicos.
- Se o grupo contiver máquinas atribuídas, especifique o número máximo de desktops por usuário. Este deve ser um valor de um ou maior.
- Habilite ou desabilite o desktop (para máquinas agrupadas) ou a regra de atribuição de desktop (para máquinas atribuídas). Desabilitar um desktop interrompe a entrega do desktop. Desabilitar uma regra de atribuição de desktop interrompe a atribuição automática de desktop aos usuários.
- Quando terminar com a caixa de diálogo, clique em **OK**.

### Número máximo de instâncias de um desktop em um site (somente PowerShell)

Para configurar o número máximo de instâncias de um desktop no site (somente PowerShell):

- No PowerShell, use o cmdlet BrokerEntitlementPolicyRule apropriado com o parâmetro MaxPerEntitlementInstances. Por exemplo, o cmdlet a seguir modifica a regra `tsvda-desktop` para definir o número máximo de instâncias simultâneas de um desktop permitidas no site para dois. Quando há duas instâncias de desktop em execução, ocorre um erro se um terceiro assinante tentar iniciar um desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- Para obter orientação, use o cmdlet Get-Help. Por exemplo, `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`.

### Etapa 7. Resumo

Insira um nome para o grupo de entrega. Você também pode (opcionalmente) inserir uma descrição, que aparece no aplicativo Citrix Workspace e no Web Studio.

Revise as informações de resumo e clique em **Concluir**.

# Gerenciar grupos de entrega

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

## Introdução

Este artigo descreve os procedimentos para gerenciar grupos de entrega a partir do console de gerenciamento. Além de alterar as configurações especificadas ao criar o grupo, você pode configurar outras configurações que não estão disponíveis ao criar um grupo de entrega.

As categorias de procedimento incluem: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Impedir que os usuários se conectem a máquinas" é descrito na categoria de máquinas, mas também afeta os usuários. Se você não conseguir encontrar uma tarefa em uma categoria, verifique uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Aplicativos contêm informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer as permissões da função interna de Administrador de Grupo de Entrega. Para obter detalhes, consulte Administração delegada.

## Geral

- Exibir detalhes do grupo
- Alterar o tipo de entrega
- Alterar endereços do StoreFront™
- Alterar o nível funcional

- Gerenciar grupos de entrega do Acesso Remoto para PC
- Organizar grupos de entrega usando pastas
- Gerenciar Proteção de Aplicativos

### Exibir detalhes do grupo

1. Use a função de pesquisa para localizar um grupo de entrega específico. Consulte Pesquisar instâncias para obter instruções.
2. Nos resultados da pesquisa, selecione um grupo conforme necessário.
3. Consulte a tabela a seguir para obter descrições das colunas do grupo.
4. Clique em uma guia no painel de detalhes inferior para obter mais informações sobre este grupo.

| COLUNA | DESCRIÇÃO |
|---|---|
| Grupo de Entrega | O nome do grupo e o tipo de sessão. Os tipos de sessão incluem SO de sessão única e SO de múltiplas sessões. |
| Entregando | O tipo de recursos entregues por este grupo. Os valores possíveis incluem Aplicativos, Desktops e Aplicativos e Desktops. "Atribuição de máquina estática" aparece se o grupo de entrega consistir em máquinas dedicadas. |
| Sessão em Uso | O número de máquinas configuradas e o número de máquinas que estão no estado Desconectado. |
| Contagem Alocada | O número de máquinas no catálogo atribuídas a um grupo de entrega. |
| Pasta | O local do grupo na árvore de **Grupos de Entrega**. Ele exibe o nome da pasta em que o grupo está (incluindo a barra invertida final), ou `-` se o grupo estiver no nível raiz. |

### Alterar o tipo de entrega de um grupo de entrega

O tipo de entrega indica o que o grupo pode entregar: aplicativos, desktops ou ambos.

Antes de alterar um tipo de **somente aplicativo** ou **desktops e aplicativos** para o tipo de **somente desktops**, exclua todos os aplicativos do grupo.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Tipo de Entrega**, selecione o tipo de entrega desejado.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

### Alterar endereços do StoreFront

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **StoreFront**, selecione ou adicione URLs do StoreFront. Essas URLs são usadas pelo aplicativo Citrix Workspace™, que é instalado em cada máquina no grupo de entrega.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Você também pode especificar endereços de servidor StoreFront selecionando **StoreFront** no painel esquerdo.

### Alterar o nível funcional

Altere o nível funcional do grupo de entrega depois de atualizar os VDAs em suas máquinas e os catálogos de máquinas que contêm as máquinas usadas no grupo de entrega.

Antes de começar:

- Se você usa o Citrix Provisioning™ (anteriormente Provisioning Services), atualize a versão do VDA no console do Citrix Provisioning.
- Inicie as máquinas que contêm o VDA atualizado para que elas possam se registrar em um Delivery Controller. Esse processo informa ao console o que precisa ser atualizado no grupo de entrega.
- Se você precisar continuar a usar versões anteriores do VDA, os recursos mais recentes do produto não estarão disponíveis. Para obter mais informações, consulte a documentação de atualização.

Para alterar o nível funcional de um grupo de entrega:

1. Selecione **Grupos de Entrega** no painel esquerdo.

2. Selecione um grupo e clique em **Alterar Nível Funcional** na barra de ações. A ação **Alterar Nível Funcional** aparece somente se VDAs atualizados forem detectados.
3. Clique em **Alterar**.

A exibição indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Você pode então cancelar a ação de alteração, resolver os problemas da máquina e, em seguida, executar a ação de alteração novamente.

Após a conclusão da alteração, você pode reverter as máquinas para seus estados anteriores. Selecione o grupo de entrega e, em seguida, selecione **Desfazer Alteração de Nível Funcional** na barra de ações.

### Gerenciar grupos de entrega do Remote PC Access

Se uma máquina em um catálogo de máquinas de Acesso Remoto para PC não for atribuída, a máquina será temporariamente atribuída a um grupo de entrega associado a esse catálogo. Essa atribuição temporária permite que a máquina seja atribuída a um usuário posteriormente.

A associação de grupo de entrega a catálogo de máquinas tem um valor de prioridade. A prioridade determina o grupo de entrega atribuído à máquina quando ela se registra no sistema ou quando um usuário precisa de uma atribuição de máquina. Quanto menor o valor, maior a prioridade. Se um catálogo de máquinas de Acesso Remoto para PC tiver várias atribuições de grupo de entrega, o software selecionará a correspondência com a prioridade mais alta. Use o SDK do PowerShell para definir esse valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas de Acesso Remoto para PC são associados a um grupo de entrega. Contas de máquina ou Unidades Organizacionais adicionadas ao catálogo posteriormente podem ser adicionadas ao grupo de entrega. Essa associação pode ser desativada ou ativada.

Para adicionar ou remover uma associação de catálogo de máquinas do Remote PC Access com um grupo de entrega:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo do Remote PC Access.
3. Na seção **Detalhes**, clique na guia **Catálogos de Máquinas** e selecione um catálogo de Acesso Remoto para PC.
4. Para adicionar ou restaurar uma associação, clique em **Adicionar Desktops**. Para remover uma associação, clique em **Remover Associação**.

## Organizar grupos de entrega usando pastas

Você pode criar pastas para organizar grupos de entrega para facilitar o acesso.

### Funções necessárias

Por padrão, você precisa ter a seguinte função interna para criar e gerenciar pastas de grupo de entrega: Administrador de Nuvem, Administrador Completo ou Administrador de Grupo de Entrega. Se necessário, você pode personalizar as funções para criar e gerenciar pastas de grupo de entrega. Para obter mais informações, consulte Permissões necessárias.

### Criar uma pasta de grupo de entrega

Antes de começar, planeje como organizar seus grupos de entrega. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de entrega e subpastas.
- Todos os nós no Web Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Grupos de Entrega**, você deve adicionar os metadados `ContainsDeliveryGroups` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

Para criar uma pasta de grupo de entrega, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra **Ação**.
3. Insira um nome para a nova pasta e, em seguida, clique em **Concluído**.

**Dica:**

> Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

### Mover um grupo de entrega

Você pode mover um grupo de entrega entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Visualize os grupos por pasta. Você também pode ativar **Ver todos** acima da hierarquia de pastas para visualizar todos os grupos de uma vez.
3. Clique com o botão direito do mouse em um grupo e, em seguida, selecione **Mover Grupo de Entrega**.
4. Selecione a pasta para a qual deseja mover o grupo e, em seguida, clique em **Concluído**.

> **Dica:**

> Você pode arrastar um grupo para uma pasta.

### Gerenciar pastas de grupos de entrega

Você pode excluir, renomear e mover pastas de grupos de entrega.

Esteja ciente de que você só pode excluir uma pasta se ela e suas subpastas não contiverem grupos de entrega.

Para gerenciar uma pasta, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

#### Permissões necessárias

A tabela a seguir lista as permissões necessárias para executar ações em pastas de grupos de entrega.

| AÇÃO | PERMISSÕES NECESSÁRIAS |
|---|---|
| Criar pastas de grupos de entrega | Criar Pasta de Grupo de Entrega |
| Excluir pastas de grupo de entrega | Remover Pasta de Grupo de Entrega |
| Mover pastas de grupo de entrega | Mover Pasta de Grupo de Entrega |
| Renomear pastas de grupo de entrega | Editar Pasta de Grupo de Entrega |
| Mover grupos de entrega para pastas | Editar Pasta de Grupo de Entrega e Editar Propriedades do Grupo de Entrega |

### Gerenciar Proteção de Aplicativos

As informações a seguir são complementares ao artigo de proteção de aplicativos em `<https://docs.citrix.com/pt-br/citrix-workspace-app/app-protection.html>`. Observe os seguintes detalhes:

- Você deve ter um direito de Proteção de Aplicativos válido. Para adquirir o recurso Proteção de Aplicativos, entre em contato com seu representante de vendas da Citrix.
- A Proteção de Aplicativos requer confiança XML. Para habilitar a confiança XML, vá para **Configurações > Habilitar confiança XML**.
- Em relação à captura anti-tela:
  - No Windows e macOS, apenas a janela do conteúdo protegido fica em branco. A Proteção de Aplicativos está ativa quando uma janela protegida não está minimizada.
  - No Linux, a captura inteira fica em branco. A Proteção de Aplicativos está ativa, esteja uma janela protegida minimizada ou não.

Para escolher um método de Proteção de Aplicativos para um grupo de entrega, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Proteção de Aplicativos**, você pode habilitar **Anti-keylogging** e **Anti-captura de tela**.

## Usuários

- Alterar configurações do usuário

- Adicionar ou remover usuários

### Alterar configurações do usuário em um grupo de entrega

O nome desta página aparece como **Configurações do Usuário** ou **Configurações Básicas**.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Configurações do Usuário** (ou **Configurações Básicas**), altere qualquer uma das configurações na tabela a seguir.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

| CONFIGURAÇÃO | DESCRIÇÃO |
|---|---|
| Descrição | O texto que o Citrix Workspace (ou StoreFront) usa e que os usuários veem. |
| Habilitar grupo de entrega | Se o grupo de entrega está habilitado. |
| Fuso horário | O fuso horário em que as máquinas deste grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site. **Nota:** Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção. |
| Habilitar Secure ICA® | Protege as comunicações de e para as máquinas no grupo de entrega usando SecureICA, que criptografa o protocolo ICA. O nível padrão é de 128 bits. O nível pode ser alterado usando o SDK. A Citrix recomenda usar mais métodos de criptografia, como a criptografia TLS, ao atravessar redes públicas. Além disso, o SecureICA não verifica a integridade dos dados. |

### Adicionar ou remover usuários em um grupo de entrega

Para obter informações detalhadas sobre usuários, consulte Usuários.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Usuários**:
   - Para adicionar usuários, clique em **Adicionar** e, em seguida, especifique os usuários que deseja adicionar.
   - Para remover usuários, selecione um ou mais usuários e clique em **Remover**.
   - Marque ou desmarque a caixa de seleção para permitir o acesso por usuários não autenticados.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

### Importar ou exportar listas de usuários

Para grupos de entrega que contêm máquinas de SO de sessão única físicas, você pode importar informações de usuário de um arquivo .csv depois de criar o grupo de entrega. Você também pode exportar informações de usuário para um arquivo .csv. O arquivo .csv pode conter dados de uma versão anterior do produto.

A primeira linha no arquivo CSV deve conter dois cabeçalhos de coluna, separados por uma vírgula. Certifique-se de que o primeiro cabeçalho seja `Machine Account` e o segundo cabeçalho seja `User Names`. (Você pode incluir cabeçalhos adicionais, mas eles não são suportados.) As linhas subsequentes no arquivo contêm dados separados por vírgulas. As entradas `Machine Account` podem ser SID do computador, FQDN ou pares de domínio e nome do computador.

Para importar ou exportar informações do usuário:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Alocação de Máquina**, selecione **Importar** lista ou **Exportar** lista e, em seguida, navegue até o local do arquivo.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

## Máquinas

- Alterar atribuições de máquinas a 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
- Restringir acesso a máquinas
- Impedir que usuários se conectem a uma máquina (modo de manutenção)
- Desligar e reiniciar máquinas
- Criar e gerenciar agendamentos de reinício para máquinas
- Habilitar agendamento de reinicialização única
- Carregar máquinas gerenciadas
- Gerenciar energia de máquinas gerenciadas

### Alterar atribuições de máquinas a usuários em um grupo de entrega

Você pode alterar as atribuições de máquinas de SO de sessão única provisionadas com MCS. Você não pode alterar as atribuições para máquinas de SO de várias sessões ou máquinas provisionadas com Citrix Provisioning.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Desktops** ou **Regras de Atribuição de Desktop** (o título da página depende do tipo de catálogo de máquinas que o grupo de entrega usa), especifique os novos usuários.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

### Alterar o número máximo de máquinas por usuário em um grupo de entrega

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Regras de Atribuição de Desktop**, defina o valor máximo de desktops por usuário.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

### Atualizar uma máquina em um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.

2. Selecione um grupo e clique em **View Machines** na barra de ações.
3. Selecione uma máquina e clique em **Update Machines** na barra de ações.

Para escolher uma imagem diferente, selecione **Imagem** e, em seguida, selecione um instantâneo.

Para aplicar as alterações e notificar os usuários da máquina, selecione **Notificação de lançamento para usuários finais**. Em seguida, especifique:

- Quando atualizar a imagem mestre: agora ou na próxima reinicialização
- O tempo de distribuição da reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados da reinicialização
- A mensagem que os usuários recebem

### Adicionar, alterar ou remover uma restrição de tag para um desktop

Adicionar, alterar e remover restrições de tag podem ter efeitos não antecipados sobre quais desktops são considerados para inicialização. Revise as considerações e precauções em Tags.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Desktops**, selecione o desktop e clique em **Editar**.
4. Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag.
5. Para alterar ou remover uma restrição de tag, faça o seguinte:
    - Selecione uma tag diferente.
    - Remova a restrição de tag desmarcando **Restringir inicializações a máquinas com esta tag**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

### Remover uma máquina de um grupo de entrega

Remover uma máquina a exclui de um grupo de entrega. Isso não a exclui do catálogo de máquinas que o grupo de entrega usa. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes de serem removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto você a remove, coloque a máquina 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 **View Machines** na barra de ações.
3. Certifique-se de que a máquina esteja desligada.
4. Selecione a máquina e clique em **Remove from Delivery Group** na barra de ações.

Você também pode remover uma máquina de um grupo de entrega através da conexão que a máquina usa.

### Restringir o acesso a máquinas em um grupo de entrega

Quaisquer alterações feitas para restringir o acesso a máquinas em um grupo de entrega substituem as configurações anteriores, independentemente do método usado. Você pode:

- **Restringir o acesso para 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 apenas a determinados aplicativos. Para obter detalhes, consulte Administração delegada.
- **Restringir acesso para usuários através de expressões de política SmartAccess:** Use expressões de política para filtrar conexões de usuário feitas através do Citrix Gateway.

  a. Selecione **Delivery Groups** no painel esquerdo.

  b. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.

  c. Na página **Access Policy**, selecione **Connections through NetScaler® Gateway**.

  d. Para escolher um subconjunto dessas conexões, selecione **Connections meeting any of the following filters**. Em seguida, defina o site do Citrix Gateway e adicione, edite ou remova as expressões de política SmartAccess para os cenários de acesso de usuário permitidos. Para obter detalhes, consulte a documentação do Citrix Gateway.

  e. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Save** para aplicar as alterações e fechar a janela.

- **Restringir acesso para usuários através de filtros de exclusão:** Use filtros de exclusão em políticas de acesso que você define no SDK. As políticas de acesso são aplicadas a grupos de entrega para refinar as conexões. Por exemplo, você pode restringir o acesso à máquina a um subconjunto de usuários e pode especificar dispositivos de usuário permitidos. Os filtros de exclusão refinam ainda mais as políticas de acesso. Por exemplo, por segurança, você pode negar acesso a um subconjunto de usuários ou dispositivos. Por padrão, os filtros de exclusão estão desabilitados.

  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 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_*` aplica o filtro a ambas as máquinas.

  Se você estiver conectado usando um navegador da web ou com o recurso de experiência do usuário do aplicativo Citrix Workspace habilitado 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 você precisa interromper temporariamente novas conexões com máquinas, pode ativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega. Você pode fazer isso antes de aplicar patches ou usar ferramentas de gerenciamento.

- Quando uma máquina de SO multi-sessão está no modo de manutenção, os usuários podem se conectar a sessões existentes, mas não podem iniciar novas sessões.
- Quando uma máquina de SO de sessão única (ou um PC usando Acesso Remoto a PC) está no modo de manutenção, os usuários não podem se conectar ou reconectar. As conexões atuais permanecem conectadas até que se desconectem ou façam logoff.

Para ativar ou desativar o modo de manutenção:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo.

3. Para ativar o modo de manutenção para todas as máquinas no grupo de entrega, clique em **Turn On Maintenance Mode** na barra de ações.

   Para ativar o modo de manutenção para uma máquina, clique em **View Machines** na barra de ações. Selecione uma máquina e, em seguida, clique em **Turn On Maintenance Mode** na barra de ações.
4. Para desativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega, siga as instruções anteriores, mas clique em **Turn Off Maintenance Mode** na barra de ações.

As configurações da Conexão de Área de Trabalho Remota (RDC) do Windows também afetam se uma máquina de SO de várias sessões está no modo de manutenção. O modo de manutenção é ativado quando ocorre qualquer um dos seguintes:

- O modo de manutenção está ativado, conforme descrito anteriormente.
- A RDC está configurada para **Não permitir conexões a este computador**.
- O RDC não está definido como **Don't allow connections to this computer**. A configuração **Remote Host Configuration User Logon Mode** é **Allow reconnections, but prevent new logons** ou **Allow reconnections, but prevent new logons until the server is restarted**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, o que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, o que afeta as máquinas nesse catálogo.

### Desligar e reiniciar máquinas em um grupo de entrega

Este procedimento não é suportado para máquinas de Acesso Remoto a PC.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Exibir Máquinas** na barra de ações.
3. Selecione a máquina e clique em uma das seguintes entradas na barra de ações:

   - **Forçar desligamento:** Desliga a máquina à força e atualiza a lista de máquinas.
   - **Reiniciar:** Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a máquina permanecerá em seu estado atual.
   - **Forçar reinício:** Desliga o sistema operacional à força e, em seguida, reinicia a máquina.
   - **Suspender:** Pausa a máquina sem desligá-la e atualiza a lista de máquinas.

- **Desligar:** Solicita ao sistema operacional que seja desligado.

Para ações não forçadas, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

A Citrix recomenda que você impeça que os usuários de máquinas de SO de sessão única selecionem **Desligar** dentro de uma sessão. Consulte a documentação da política da Microsoft para obter detalhes.

Você também pode desligar e reiniciar máquinas em uma conexão.

### Criar e gerenciar agendamentos de reinicialização para máquinas em um grupo de entrega

> **Nota:**
>
> - Quando um agendamento de reinicialização é aplicado a um grupo de entrega com Autoscale™ ativado, suas máquinas são apenas desligadas e deixadas para o Autoscale ligá-las.
> - Quando os agendamentos de reinicialização são aplicados a máquinas aleatórias de sessão única, essas máquinas são desligadas em vez de reiniciadas, para economizar custos. Recomendamos que você use o Autoscale para ligar as máquinas.
> - Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

Um agendamento de reinicialização especifica quando as máquinas em um grupo de entrega são reiniciadas periodicamente. Você pode criar um ou mais agendamentos para um grupo de entrega. Um agendamento pode afetar:

- Todas as máquinas do grupo.
- Uma ou mais (mas não todas) máquinas no grupo. As máquinas são identificadas por uma tag que você aplica à máquina. Isso é chamado de restrição de tag, porque a tag restringe uma ação apenas a itens que possuem a tag.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você deseja que todas as máquinas sejam reiniciadas uma vez por semana e que as máquinas usadas pela equipe de contabilidade sejam reiniciadas diariamente. Para conseguir isso, configure um agendamento para todas as máquinas e outro agendamento apenas para as máquinas da contabilidade.

Um agendamento inclui o dia e a hora em que a reinicialização começa e a duração.

Você pode ativar ou desativar um agendamento. Desativar um agendamento pode ser útil durante testes, em intervalos especiais ou ao preparar agendamentos antes de precisar deles.

Você não pode usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reiniciar.

### Sobreposição de agendamentos

Vários agendamentos podem se sobrepor. No exemplo acima, ambos os agendamentos afetam as máquinas de contabilidade. Essas máquinas podem ser reiniciadas duas vezes no domingo. O código de agendamento foi projetado para evitar reiniciar a mesma máquina com mais frequência do que o pretendido, mas isso não pode ser garantido.

- Se os agendamentos coincidirem precisamente nos horários de início e duração, é mais provável que as máquinas sejam reiniciadas apenas uma vez.
- Quanto mais os agendamentos diferirem nos horários de início e duração, mais provável é que ocorram várias reinicializações.
- O número de máquinas afetadas por um agendamento também afeta a chance de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário para máquinas de contabilidade, dependendo da duração especificada para cada um.

Para uma análise aprofundada dos agendamentos de reinicialização, consulte Detalhes internos do agendamento de reinicialização.

### Exibir agendamentos de reinicialização

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Selecione a página **Agendamento de Reinicialização**.

A página **Agendamento de Reinicialização** contém as seguintes informações para cada agendamento configurado:

- Nome do agendamento.
- Restrição de tag usada, se houver.
- Com que frequência as reinicializações da máquina ocorrem.
- Se os usuários da máquina recebem uma notificação.
- Se o agendamento está ativado.

### Adicionar (aplicar) tags

Ao configurar um agendamento de reinicialização que usa uma restrição de tag, certifique-se de que a tag foi adicionada às máquinas que o agendamento afeta. No exemplo acima, cada uma das máquinas usadas pela equipe de contabilidade tem uma tag aplicada. Para obter detalhes, consulte Tags.

Embora você possa aplicar mais de uma tag a uma máquina, um agendamento de reinicialização pode especificar apenas uma tag.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo que contém as máquinas controladas pelo agendamento.
3. Clique em **Exibir Máquinas** e selecione as máquinas às quais deseja adicionar uma tag.
4. Clique em **Gerenciar Tags** na barra de ações.
5. Se a tag existir, marque a caixa de seleção ao lado do nome da tag. Se a tag não existir, clique em **Criar** e especifique o nome da tag. Depois que a tag for criada, marque a caixa de seleção ao lado do nome da tag recém-criada.
6. Clique em **Salvar** na caixa de diálogo **Gerenciar Tags**.

### Criar um agendamento de reinicialização

> **Nota:**
>
> Os agendamentos de reinício podem ser aplicados a todas as máquinas multissessão gerenciadas por energia e não gerenciadas por energia.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Agendamento de Reinicialização**, clique em **Adicionar**.
4. Na página **Add Restart Schedule**:

- Para habilitar o agendamento, selecione **Yes**. Para desabilitar o agendamento, selecione **No**.
- Digite um nome e uma descrição para o agendamento.
- Para **Restrict to tag**, aplique uma restrição de tag.
- Para **Include machines in maintenance mode**, escolha se deseja incluir máquinas que estão no modo de manutenção neste agendamento. Para usar o PowerShell, consulte Reinicializações agendadas para máquinas em modo de manutenção.
- Para **Restart frequency**, selecione a frequência com que a reinicialização ocorre: diariamente, semanalmente, mensalmente ou uma vez. Se você selecionar **Weekly** ou **Monthly**, poderá especificar um ou mais dias específicos.
- Para **Repeats every**, especifique a frequência com que você deseja que o agendamento seja executado.
- Para **Start date**, especifique uma data de início para a primeira ocorrência do agendamento.
- Para **Begin restart at**, especifique, no formato de 24 horas, a hora do dia para iniciar a reinicialização.
- Para **Restart duration**:
  - Se você não quiser usar a reinicialização natural, selecione **Reiniciar todas as máquinas ao mesmo tempo** ou **Reiniciar todas as máquinas dentro de um período**.
  - Se você quiser usar a reinicialização natural, selecione **Reiniciar todas as máquinas após o esgotamento de todas as sessões**.

    Ao iniciar um agendamento de reinicialização configurado para usar a reinicialização natural:

    - Todas as máquinas ociosas pertencentes ao grupo de entrega são reiniciadas imediatamente
    - Cada máquina pertencente a um grupo de entrega com uma ou mais sessões ativas é reiniciada quando todas as sessões são desconectadas.

> **Nota:**

> Os agendamentos de reinicialização natural só podem reiniciar máquinas gerenciadas por energia.

- Em **Enviar notificação aos usuários**, escolha se deseja exibir uma mensagem de notificação nas máquinas aplicáveis antes do início de uma reinicialização. Por padrão, nenhuma mensagem aparece.
- Se você optar por exibir uma mensagem 15 minutos antes do início da reinicialização, poderá escolher (em **Frequência de notificação**) repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não se repete.
- Insira o título e o texto da notificação. Não há texto padrão.

  Se você quiser que a mensagem inclua uma contagem regressiva para o reinício, inclua a variável **%m%**. A menos que você tenha escolhido reiniciar todas as máquinas ao mesmo tempo, a mensagem aparecerá em cada máquina no momento apropriado antes do reinício.

5. Clique em **Concluído** para aplicar as alterações e fechar a janela **Adicionar Agendamento de Reinício**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Salvar** para aplicar as alterações e fechar a janela.

### Reiniciar após o esgotamento

Outro valor de duração de reinício está disponível ao usar o PowerShell para criar ou atualizar um agendamento de reinício de máquina (`New-BrokerRebootSchedulev2` ou `Set-BrokerRebootSchedulev2`).

Ao habilitar o recurso de reinício após o esvaziamento com o parâmetro `-UseNaturalReboot <Boolean>`, todas as máquinas são reiniciadas após o esvaziamento de todas as sessões. Quando o tempo de reinício é atingido, as máquinas são colocadas no estado de esvaziamento e, em seguida, reiniciadas quando todas as sessões são encerradas.

Este recurso é compatível com grupos de entrega que contêm máquinas de sessão única ou multi-sessão. Você pode usar esta opção para máquinas que são gerenciadas por energia e também para máquinas que não são gerenciadas por energia.

Em um ambiente local, este recurso é suportado apenas ao usar o PowerShell. O recurso não está disponível no Web Studio.

### Editar, remover, ativar ou desativar um agendamento de reinicialização

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Reiniciar Agendamento**, selecione a caixa de seleção de um agendamento.
    - Para editar um agendamento, clique em **Editar**. Atualize a configuração do agendamento, usando as orientações em Criar um agendamento de reinício.
    - Para habilitar ou desabilitar um agendamento, clique em **Editar**. Selecione ou desmarque a caixa de seleção **Habilitar agendamento de reinício**.
    - Para remover um agendamento, clique em **Remover**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma tag aplicada às máquinas nas máquinas afetadas.

### Reinicializações agendadas atrasadas devido a interrupção do banco de dados

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

> Se ocorrer uma interrupção do banco de dados do site antes do início de um reinício agendado para máquinas (VDAs) em um grupo de entrega, os reinícios começarão quando a interrupção terminar. Isso pode ter resultados indesejados.

Por exemplo, digamos que você agendou os reinícios de um grupo de entrega para ocorrerem fora do horário de produção (começando às 03:00). Ocorre uma interrupção do banco de dados do site uma hora antes do início de um reinício agendado (02:00). A interrupção dura seis horas (até as 08:00). O agendamento de reinício começa quando a conexão entre o Delivery Controller e o banco de dados do site é restaurada. Os reinícios dos VDAs agora começam cinco horas após o agendamento original, resultando em VDAs reiniciando durante o horário de produção.

Para ajudar a evitar essa situação, você pode usar o parâmetro `MaxOvertimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além do horário de início agendado em que um agendamento de reinicialização pode começar.

- Se a conexão do banco de dados for restaurada dentro desse tempo (horário agendado + `MaxOvertimeStartMins`), as reinicializações do VDA começarão.

- Se a conexão do banco de dados não for restaurada dentro desse tempo, as reinicializações do VDA não começarão.
- Se este parâmetro for omitido ou tiver um valor zero, a reinicialização agendada começará quando a conexão com o banco de dados for restaurada, independentemente da duração da interrupção.

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell. Você não pode definir este valor ao configurar um agendamento de reinício no Web Studio.

#### Reinicializações agendadas para máquinas em modo de manutenção

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell. A opção `IgnoreMaintenanceMode` é compatível com Citrix Virtual Apps and Desktops 7 2006 e posterior.

> Para indicar se um agendamento de reinício afeta máquinas que estão em modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria um agendamento que reinicia máquinas que estão em modo de manutenção (além das máquinas que não estão em modo de manutenção).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

O cmdlet a seguir modifica um agendamento de reinicialização existente.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell.

### Habilitar agendamento de reinício único

Se você quiser habilitar um agendamento de reinicialização único usando o PowerShell, use os seguintes comandos `BrokerCatalogRebootSchedule` do PowerShell para criar, modificar e excluir um agendamento de reinicialização:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Limitações:

- Um agendamento de reinicialização de catálogo associado a um catálogo sem um fuso horário configurado é criado, mas não é iniciado.
- Quando um agendamento de reinicialização de catálogo é criado, o agendamento de reinicialização é executado apenas nas VMs do catálogo que pertencem a um grupo de entrega.

Exemplo,

- Para criar um agendamento de reinicialização das VMs no catálogo chamado **BankTellers** para começar em Feb 3, 2022, entre 2h e 4h.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- Para criar um agendamento de reinicialização das VMs no catálogo com UID 17 para começar em Feb 3, 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM é configurada para exibir uma caixa de mensagem com o título **AVISO: Reinicialização pendente** e a mensagem **Salve seu trabalho**, em cada sessão de usuário.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- Para renomear o agendamento de reinicialização do catálogo de **Old Name** para **New Name**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- Para exibir todos os agendamentos de reinicialização de catálogo com UID 1 e, em seguida, renomear o agendamento de reinicialização de catálogo com UID 1 para **New Name**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Para definir o agendamento de reinicialização do catálogo chamado **Contabilidade** para exibir uma mensagem com o título **AVISO: Reinicialização pendente e a mensagem Salve seu trabalho**, dez minutos antes da reinicialização de cada VM. A mensagem aparece em cada sessão de usuário nessa VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- Para exibir todos os agendamentos de reinicialização desabilitados e, em seguida, habilitar todos os agendamentos de reinicialização desabilitados.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- Para definir o agendamento de reinicialização do catálogo com UID 17 para exibir a mensagem **Reiniciando em %m% minutos** quinze, dez e cinco minutos antes da reinicialização de cada VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- Para configurar o fuso horário para o catálogo chamado **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

### Gerenciar carga de máquinas em grupos de entrega

Você pode gerenciar a carga apenas de máquinas de SO de várias sessões.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as condições ambientais atuais. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** Uma máquina de SO de várias sessões é considerada para balanceamento de carga apenas quando o modo de manutenção está desativado.
- **Índice de carga do servidor:** Determina a probabilidade de um servidor que entrega máquinas de SO de várias sessões receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações para métricas de desempenho, como uso de CPU, disco e memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga.

  Um índice de carga do servidor de 10000 indica que o servidor está totalmente carregado. Se nenhum outro servidor estiver disponível, os usuários poderão receber uma mensagem de que a área de trabalho ou o aplicativo está indisponível ao iniciar uma sessão.

  Você pode monitorar o índice de carga no Director (Monitor), na pesquisa do Web Studio (Gerenciar) e no SDK.

  Nas exibições do console, para exibir a coluna **Índice de Carga do Servidor** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse em um cabeçalho de coluna e selecione **Selecionar Coluna**. Na **categoria Máquina**, selecione **Índice de Carga**.

  No SDK, use o cmdlet `Get-BrokerMachine`. Para obter detalhes, consulte CTX202150.
- **Configuração da política de tolerância de logon simultâneo**: O número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões do XenApp 6.x.)

  Quando todos os servidores estão no nível ou acima da configuração de tolerância de logon simultâneo, a próxima solicitação de logon é atribuída ao servidor com o menor número de logons pendentes. Se mais de um servidor atender a esses critérios, o servidor com o menor índice de carga será selecionado.

### Máquinas com gerenciamento de energia em um grupo de entrega

Você pode gerenciar a energia apenas de máquinas virtuais de SO de sessão única, não de máquinas físicas (incluindo máquinas de Acesso Remoto a PC). Máquinas de SO de sessão única com recursos de GPU não podem ser suspensas, portanto, as operações de desligamento falham. Para máquinas de SO de várias sessões, você pode criar um agendamento de reinicialização.

Em grupos de entrega que contêm máquinas agrupadas, as máquinas virtuais de SO de sessão única podem estar em um dos seguintes estados:

- Alocadas aleatoriamente e em uso
- Não alocadas e desconectadas

Em grupos de entrega que contêm máquinas estáticas, as máquinas virtuais de SO de sessão única podem ser:

- Alocadas permanentemente e em uso
- Alocadas permanentemente e desconectadas (mas prontas)
- Não alocadas e desconectadas

Durante o uso normal, os grupos de entrega estáticos geralmente contêm máquinas alocadas permanentemente e não alocadas. Inicialmente, todas as máquinas não são alocadas, exceto as alocadas manualmente quando o grupo de entrega foi criado. À medida que os usuários se conectam, as máquinas se tornam alocadas permanentemente. Você pode gerenciar totalmente a energia das máquinas não alocadas nesses grupos de entrega, mas apenas parcialmente as máquinas alocadas permanentemente.

- **Pools e buffers:** Para grupos de entrega em pool e grupos de entrega estáticos com máquinas não alocadas, um pool (neste caso) é um conjunto de máquinas não alocadas ou temporariamente alocadas que são mantidas em estado ligado, prontas para os usuários se conectarem. Um usuário obtém uma máquina imediatamente após o logon. O tamanho do pool (o número de máquinas mantidas ligadas) é configurável por hora do dia. Para grupos de entrega estáticos, use o SDK para configurar o pool.

  Um buffer é um conjunto extra de máquinas não alocadas em espera que são ligadas quando o número de máquinas no pool cai abaixo de um limite. O limite é uma porcentagem do tamanho do grupo de entrega. Para grupos de entrega grandes, um número significativo de máquinas pode ser ligado quando o limite é excedido. Portanto, planeje os tamanhos dos grupos de entrega cuidadosamente ou use o SDK para ajustar o tamanho padrão do buffer.
- **Temporizadores de estado de energia:** Você pode usar temporizadores de estado de energia para suspender máquinas depois que os usuários se desconectarem por um período de tempo especificado. Por exemplo, as máquinas são suspensas automaticamente fora do horário de expediente se os usuários estiverem desconectados por pelo menos 10 minutos.

  Você pode configurar temporizadores para dias de 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 de pico. Você não tem o controle preciso que tem com máquinas não alocadas sobre o número de máquinas que se tornam disponíveis para compensar as máquinas que são consumidas.

**Gerenciar energia de máquinas virtuais de SO de sessão única**

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** na barra de ações.
3. Na página **Gerenciamento de Energia**, selecione **Dias da semana** em **Gerenciar energia das máquinas**. Por padrão, os dias da semana são de segunda a sexta-feira.
4. Para grupos de entrega aleatórios, em **Máquinas a serem ligadas**, clique em **Editar** e especifique o tamanho do pool durante os dias da semana. Em seguida, selecione o número de máquinas a serem ligadas.
5. Em **Horas de pico**, defina as horas de pico e fora de pico para cada dia.
6. Defina os temporizadores de estado de energia para horários de pico e fora de pico durante os dias da semana: Em **Durante as horas de pico > Quando desconectado**, especifique o atraso (em minutos) antes de suspender qualquer máquina desconectada no grupo de entrega e, em seguida, selecione **Suspender**. Em **Durante as horas fora de pico > Quando desconectado**, especifique o atraso antes de desligar qualquer máquina desconectada no grupo de entrega e, em seguida, selecione **Desligar**. Este temporizador não está disponível para grupos de entrega com máquinas aleatórias.
7. Selecione **Fim de semana** em **Gerenciar energia das máquinas** e, em seguida, configure as horas de pico e os temporizadores de estado de energia para os fins de semana.
8. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Use o SDK para:

- Desligar, em vez de suspender, máquinas em resposta a temporizadores de estado de energia, ou se você quiser que os temporizadores sejam baseados em logoffs, em vez de desconexões.
- Alterar as definições padrão de dias de semana e fins de semana.
- Desativar o gerenciamento de energia. Consulte CTX217289.

**Gerenciar energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas**

> **Importante:**

> Este aprimoramento aplica-se apenas a máquinas VDI com sessões desconectadas. Não se aplica a máquinas VDI com sessões com logoff.

> Em versões anteriores, uma máquina VDI em transição para um período de tempo onde uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária, permanecia ligada. Esse cenário ocorria se a máquina se desconectasse durante um período de tempo (horários de pico ou fora de pico) onde nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir do Citrix Virtual Apps and Desktops 7 1909, a máquina é suspensa ou desligada quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega VDI:

- Defina `PeakDisconnectAction` como "Nada"
- Defina `OffPeakDisconnectAction` como "Desligar"
- Defina `OffPeakDisconnectTimeout` como "10"

Para obter mais informações sobre a ação de desconexão na política de energia, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Em versões anteriores, uma máquina VDI com uma sessão desconectada durante os horários de pico permanecia ligada quando fazia a transição do pico para o fora de pico. A partir do Citrix Virtual Apps and Desktops 7 1909, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina VDI na transição de período. Como resultado, a máquina é desligada 10 minutos depois de fazer a transição para o fora de pico.

Se você quiser reverter para o comportamento anterior (ou seja, não realizar nenhuma ação em máquinas que fazem a transição do pico para o fora de pico ou do fora de pico para o pico com sessões desconectadas), faça uma das seguintes ações:

- Defina o valor do registro `LegacyPeakTransitionDisconnectedBehaviour` como `1`, o equivalente a *true* que habilita o comportamento anterior. Por padrão, o valor é `0`, ou *false*, o que aciona as ações da política de energia de desconexão na transição de período.

  - Caminho: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Nome: `LegacyPeakTransitionDisconnectedBehaviour`
  - Tipo: `REG_DWORD`
  - Dados: `0x00000001 (1)`

- Configure a configuração usando o `Set-BrokerServiceConfigurationData` comando PowerShell. Por exemplo:

  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações da política de energia possam ser aplicadas a ela na transição de período:

- Ter uma sessão desconectada.
- Não ter ações de energia pendentes.
- Pertencer a um grupo de entrega VDI (sessão única) que transita para um período de tempo diferente.
- Ter uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e transita para um período onde uma ação de energia é atribuída.

**Alterar a porcentagem de VDAs em estado ligado para catálogos**

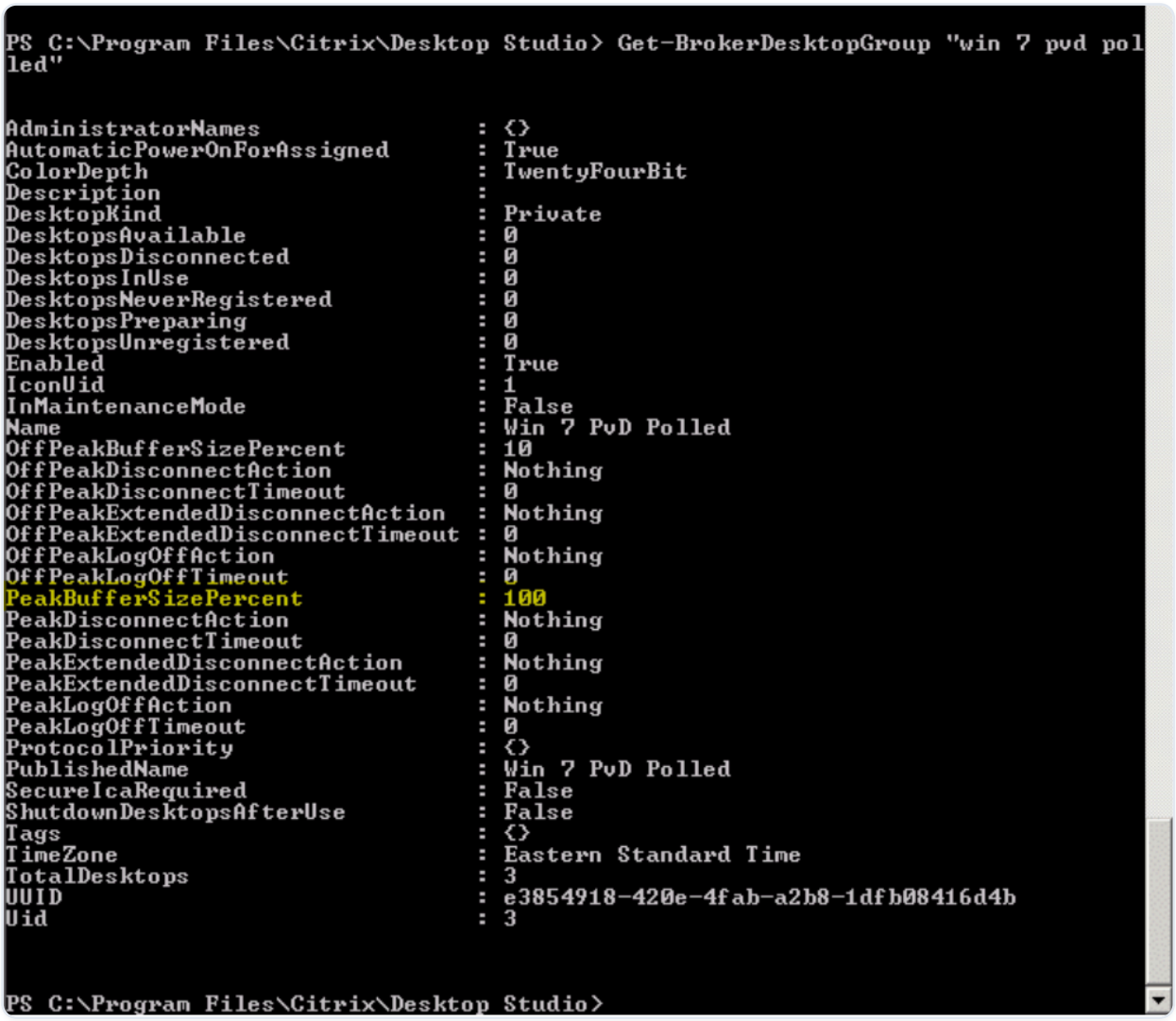
1. Ajuste os horários de pico para o grupo de entrega na seção **Gerenciamento de energia** para o grupo de entrega.
2. Anote o nome do Grupo de Área de Trabalho.
3. Com privilégios de administrador, inicie o PowerShell e execute os seguintes comandos. Substitua "Nome do Grupo de Área de Trabalho" pelo nome do seu grupo de área de trabalho que tem uma porcentagem alterada de VDAs em execução.

   `asnp Citrix*`

   `# Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100`

   Um valor de 100 significa que 100% dos VDAs estão no estado pronto.
4. Verifique a solução executando:

   `#Get-BrokerDesktopGroup "Desktop Group Name"`




Pode levar até uma hora para que as alterações entrem em vigor.

Para desligar os VDAs depois que o usuário faz logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

Para reiniciar os VDAs durante os horários de pico, para que estejam prontos para os usuários depois que eles fizerem logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

## Sessões

- Fazer logoff ou desconectar uma sessão, ou enviar uma mensagem aos usuários
- Configurar o pré-lançamento e a permanência da sessão
- Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção

- Configurar o roaming de sessão

### Fazer logoff ou desconectar uma sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** na barra de ações.
3. No painel central, selecione a máquina, selecione **View Sessions** na barra de ações e, em seguida, selecione uma sessão.
    - Alternativamente, no painel central, selecione a guia **Session** e, em seguida, selecione uma sessão.
4. Para fazer logoff de uma sessão, selecione **Log off** na barra de ações. A sessão é fechada e o usuário é desconectado. A máquina fica disponível para outros usuários, a menos que esteja alocada a um usuário específico.
5. Para desconectar uma sessão, selecione **Disconnect** na barra de ações. Os aplicativos continuam a ser executados na sessão e a máquina permanece alocada a esse usuário. O usuário pode se reconectar à mesma máquina.

Você pode configurar temporizadores de estado de energia para máquinas de SO de sessão única para manipular automaticamente sessões não utilizadas. Para obter detalhes, consulte Máquinas gerenciadas por energia.

### Enviar uma mensagem para um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** na barra de ações.
3. No painel central, selecione uma máquina para a qual você deseja enviar uma mensagem.
4. Na barra de ações, selecione **View Sessions**.
5. No painel do meio, selecione todas as sessões e, em seguida, selecione **Enviar Mensagem** na barra de ações.
6. Digite sua mensagem e clique em **OK**. Você pode especificar o nível de severidade, se necessário. As opções incluem **Crítico**, **Pergunta**, **Aviso** e **Informação**.

Alternativamente, você pode enviar uma mensagem usando o Citrix Director. Para obter mais informações, consulte Enviar mensagens para usuários.

### Configurar o pré-lançamento de sessão e a permanência de sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas de SO multi-sessão.

Os recursos de pré-lançamento de sessão e de permanência de sessão ajudam os usuários especificados a acessar aplicativos rapidamente, iniciando sessões antes que sejam solicitadas (pré-lançamento de sessão) e mantendo as sessões de aplicativo ativas depois que um usuário fecha todos os aplicativos (permanência de sessão).

Por padrão, o pré-lançamento de sessão e a permanência de sessão não são usados. Uma sessão é iniciada (lançada) quando um usuário inicia um aplicativo e permanece ativa até que o último aplicativo aberto na sessão seja fechado.

Considerações:

- O grupo de entrega deve suportar aplicativos, e as máquinas devem estar executando um VDA para SO multi-sessão, versão mínima 7.6.
- Esses recursos são suportados apenas ao usar o aplicativo Citrix Workspace para Windows e também exigem configuração extra do aplicativo Citrix Workspace. Para obter instruções, procure por pré-lançamento de sessão na documentação do produto para sua versão do aplicativo Citrix Workspace para Windows.
- O Citrix Workspace app para HTML5 não é compatível.
- Ao usar o pré-lançamento de sessão, se a máquina de um usuário for colocada em modo de suspensão ou hibernação, o pré-lançamento não funciona (independentemente das configurações de pré-lançamento de sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário sair do Citrix Workspace app, a sessão é encerrada e o pré-lançamento não se aplica mais.
- Ao usar o pré-lançamento de sessão, as máquinas cliente físicas não podem usar as funções de gerenciamento de energia de suspensão ou hibernação. Os usuários da máquina cliente podem bloquear suas sessões, mas não devem fazer logoff.
- Sessões pré-lançadas e persistentes consomem uma licença simultânea, mas apenas quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. Sessões pré-lançadas e persistentes não utilizadas são desconectadas após 15 minutos por padrão. Este valor pode ser configurado no PowerShell (cmdlet `New/Set-BrokerSessionPreLaunch`).
- O planejamento e o monitoramento cuidadosos dos padrões de atividade dos seus usuários são essenciais para adaptar esses recursos para que se complementem. A configuração ideal

equilibra os benefícios da disponibilidade antecipada de aplicativos para os usuários com o custo de manter as licenças em uso e os recursos alocados.

- Você também pode configurar o pré-lançamento de sessão para um horário agendado no Citrix Workspace app.

**Por quanto tempo as sessões pré-inicializadas e persistentes não utilizadas permanecem ativas**

Existem várias maneiras de especificar por quanto tempo uma sessão não utilizada permanece ativa se o usuário não iniciar um aplicativo: um tempo limite configurado e limites de carga do servidor. Você pode configurar todos eles. O evento que ocorre primeiro faz com que a sessão não utilizada seja encerrada.

- **Tempo limite:** Um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-lançada ou persistente não utilizada permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-lançadas terminam antes de fornecerem ao usuário o benefício de um acesso mais rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário de entrada podem ser negadas porque o servidor não tem recursos suficientes.

  Você pode habilitar esse tempo limite apenas no SDK (cmdlet `New/Set-BrokerSessionPreLaunch`), não no console de gerenciamento. Se você desabilitar o tempo limite, ele não aparecerá na exibição do console para esse grupo de entrega ou nas páginas **Editar Grupo de Entrega**.
- **Limites:** O encerramento automático de sessões pré-lançadas e persistentes com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, assumindo que os recursos do servidor estejam disponíveis. As sessões pré-lançadas e persistentes não utilizadas não causam conexões negadas porque são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

  Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-lançamento ou persistência por mais tempo são encerradas. As sessões são encerradas uma a uma em intervalos de um minuto até que a carga caia abaixo do limite. Enquanto o limite é excedido, nenhuma nova sessão de pré-lançamento é iniciada.

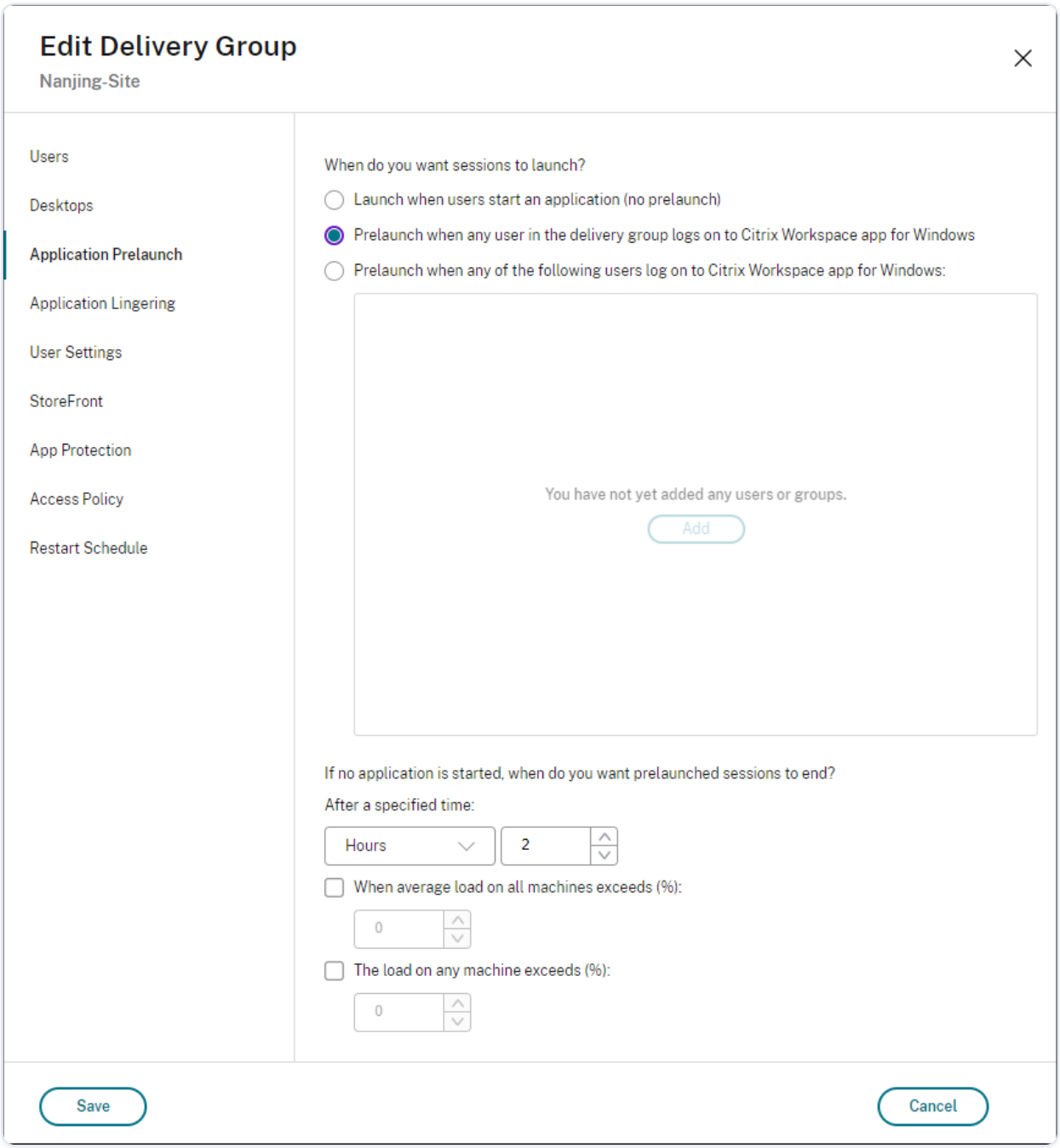
Servidores com VDAs que não se registraram em um Controller e servidores em modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com

que as sessões de pré-lançamento e persistentes sejam encerradas automaticamente para liberar capacidade.

**Para habilitar o pré-lançamento de sessão**

1. Selecione um grupo e, em seguida, clique em **Editar Grupo de Entrega** na barra de ações.
2. Na página **Pré-lançamento de Aplicativos**, ative o pré-lançamento de sessão escolhendo quando as sessões são iniciadas:

    - Quando um usuário inicia um aplicativo. Esta é a configuração padrão. O pré-lançamento de sessão está desativado.
    - Quando qualquer usuário no grupo de entrega faz logon no Citrix Workspace app para Windows.
    - Quando qualquer pessoa em uma lista de usuários e grupos de usuários faz logon no Citrix Workspace app para Windows. Certifique-se de especificar também usuários ou grupos de usuários se você escolher esta opção.



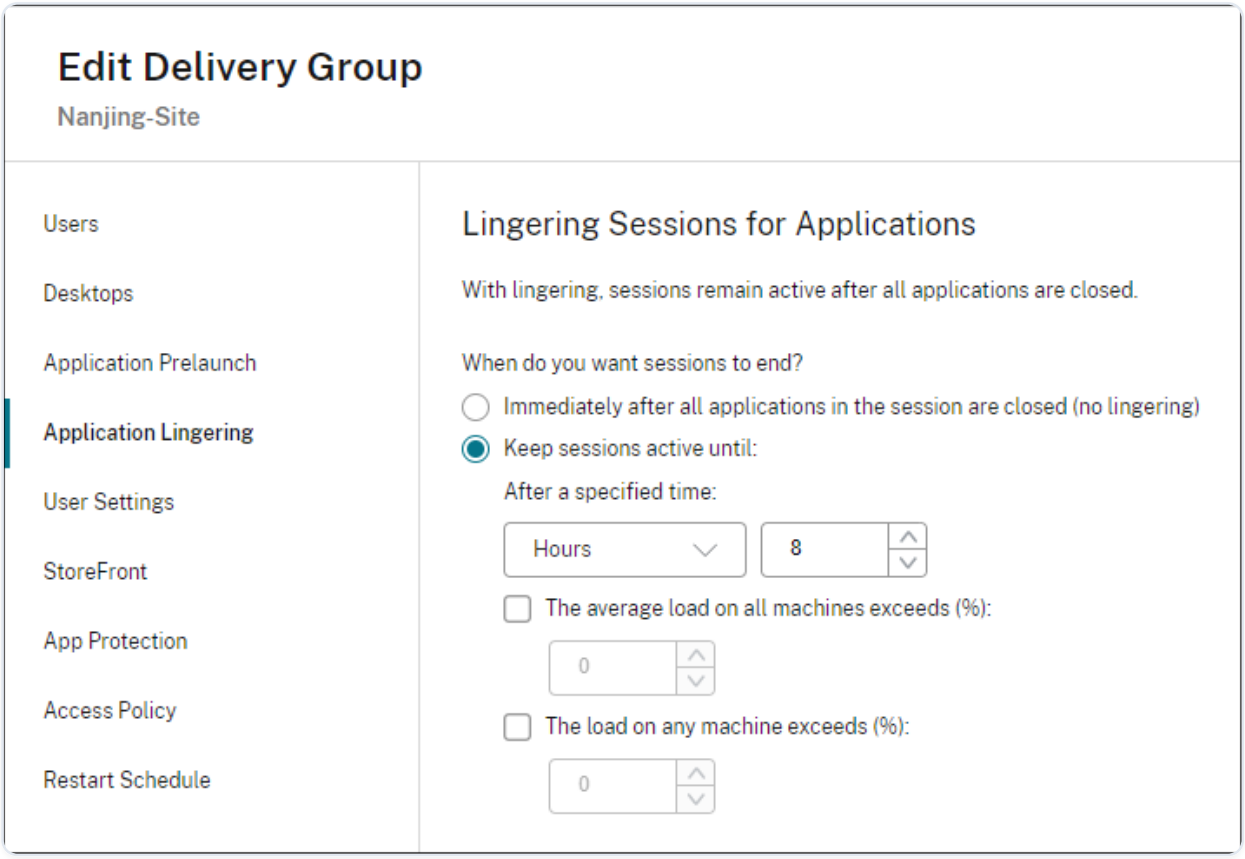

3. Uma sessão pré-lançada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-lançada não for usada), as seguintes configurações afetam por quanto tempo essa sessão permanece ativa.

   - Quando um intervalo de tempo especificado decorre. Você pode alterar o intervalo de tempo (1–99 dias, 1–2376 horas ou 1–142.560 minutos).
   - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada (1–99%).
   - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada (1–99%).

Recapitulação: Uma sessão pré-lançada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado decorre ou um limite de carga especificado é excedido.

### Para habilitar a permanência da sessão

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar Grupo de Entrega** na barra de ações.
3. Na página **Permanência do Aplicativo**, ative a permanência da sessão selecionando **Manter sessões ativas até**.




4. Várias configurações afetam por quanto tempo uma sessão persistente permanece ativa se o usuário não iniciar outro aplicativo.

   - Quando um intervalo de tempo especificado expira. Você pode alterar o intervalo de tempo: 1 a 99 dias, 1 a 2376 horas ou 1 a 142.560 minutos.
   - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada: 1 a 99%.
   - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada: 1 a 99%.

> Recapitulação: Uma sessão persistente permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado expira ou um limite de carga especificado é excedido.

### Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção

> **NOTA:**
>
> Este recurso está disponível apenas no PowerShell.
>
> Você pode controlar se as sessões que são desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes da versão 2106, a reconexão não era permitida para sessões de desktop agrupadas de sessão única que haviam sido desconectadas de máquinas 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 true, as sessões podem se reconectar às máquinas do grupo.
- Quando definido como falso, as sessões não podem se reconectar às máquinas no grupo.

Valores padrão:

- Sessão única: Desabilitado
- Multi-sessão: Habilitado

### Configurar roaming de sessão

Por padrão, o roaming de sessão está habilitado para grupos de entrega. As sessões transitam entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos estão simultaneamente disponíveis em ambos os dispositivos. Você pode visualizar os aplicativos em vários dispositivos.

Os aplicativos seguem, independentemente do dispositivo ou se existem sessões atuais. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem. Alternativamente, você pode usar o PowerShell. Para obter mais informações, consulte Roaming de sessão.

### Configurar roaming de sessão para aplicativos

Para configurar o roaming de sessão para aplicativos, siga estas etapas:

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar Grupo de Entrega** na barra de ações.
3. Na página **Usuários**, habilite o roaming de sessão selecionando a caixa de seleção **Sessões fazem roaming com os usuários à medida que eles se movem entre dispositivos**.
    - Quando habilitado, se um usuário iniciar uma sessão de aplicativo e depois se mover para outro dispositivo, a mesma sessão será usada e estará disponível em ambos os dispositivos. Quando desabilitado, a sessão não fará mais roaming entre os dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

### Configurar roaming de sessão para desktops

Para configurar o roaming de sessão para um desktop, siga estas etapas:

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Desktops**, selecione o desktop e selecione **Edit**.
4. Habilite o roaming de sessão selecionando a caixa de seleção **Session roaming**.

- Quando ativado, se o usuário iniciar o desktop e depois mudar para outro dispositivo, a mesma sessão será usada e os aplicativos estarão disponíveis em ambos os dispositivos. Quando desativado, a sessão não faz mais roaming entre os dispositivos.

Selecione **OK** para aplicar as alterações e fechar a janela.

## Solução de problemas

- VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização de recursos que, de outra forma, estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador pode solucionar. A exibição de detalhes fornece

informações de solução de problemas no assistente de criação de catálogo e depois que você adiciona um catálogo a um grupo de entrega.

Depois de criar um grupo de entrega, o painel de detalhes de um grupo de entrega indica o número de máquinas que podem ser registradas, mas não estão. Por exemplo, uma ou mais máquinas estão ligadas e não em modo de manutenção, mas não estão atualmente registradas em um Controller. Ao visualizar uma máquina "não registrada, mas deveria estar", revise a guia **Solucionar problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

Para mensagens sobre o nível funcional, consulte Versões de VDA e níveis funcionais.

Para obter informações sobre a solução de problemas de registro do VDA, consulte CTX136668.

- Na exibição de um grupo de entrega, a **versão do VDA instalada** no painel de detalhes pode ser diferente da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas com status de **Estado de Energia Desconhecido**, consulte CTX131267 para obter orientação.

# Criar grupos de aplicativos

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

## Introdução

Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Crie grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega. Ou, aplicativos usados por um subconjunto de usuários dentro de grupos de entrega. Os grupos de aplicativos são opcionais; eles oferecem uma alternativa para adicionar os mesmos aplicativos a vários grupos de entrega. Associe grupos de entrega a mais de um grupo de aplicativos e associe um grupo de aplicativos a mais de um grupo de entrega.

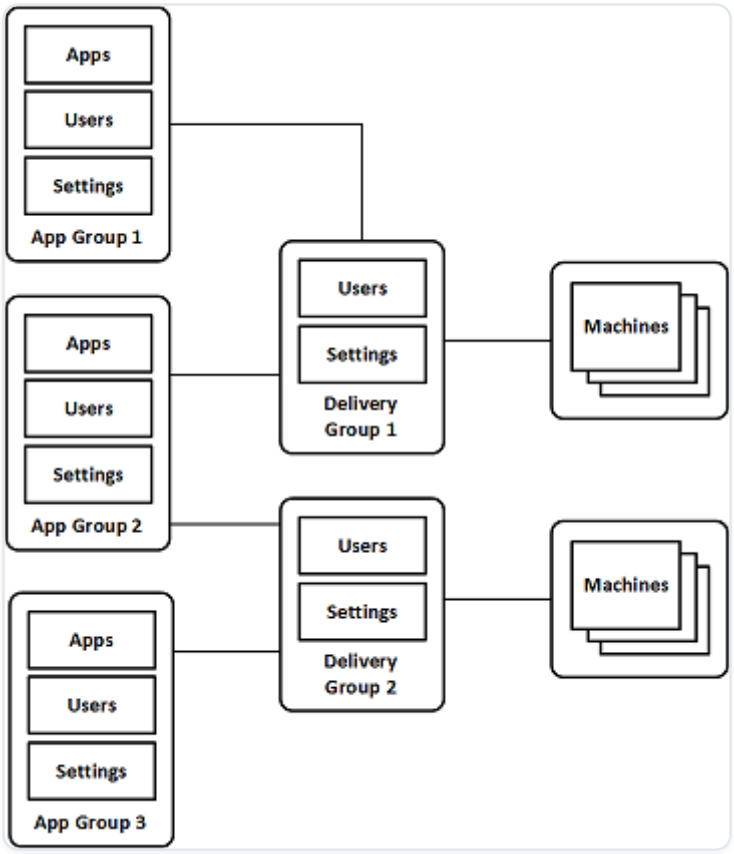
O uso de grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega:

- O agrupamento lógico de aplicativos e suas configurações permite gerenciar esses aplicativos como uma única unidade. Por exemplo, você não precisa adicionar (publicar) o mesmo aplicativo a grupos de entrega individuais um por um.
- O compartilhamento de sessão entre grupos de aplicativos pode conservar o consumo de recursos. Em outros casos, desabilitar o compartilhamento de sessão entre grupos de aplicativos pode ser benéfico.
- Você pode usar o recurso de restrição de tag para publicar aplicativos de um grupo de aplicativos, considerando apenas um subconjunto das máquinas nos grupos de entrega selecionados. Com as restrições de tag, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de máquinas extras. Uma restrição de tag pode ser pensada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

## Configurações de exemplo

**Exemplo 1:**

O gráfico a seguir mostra uma implantação do Citrix Virtual Apps and Desktops que inclui grupos de aplicativos:



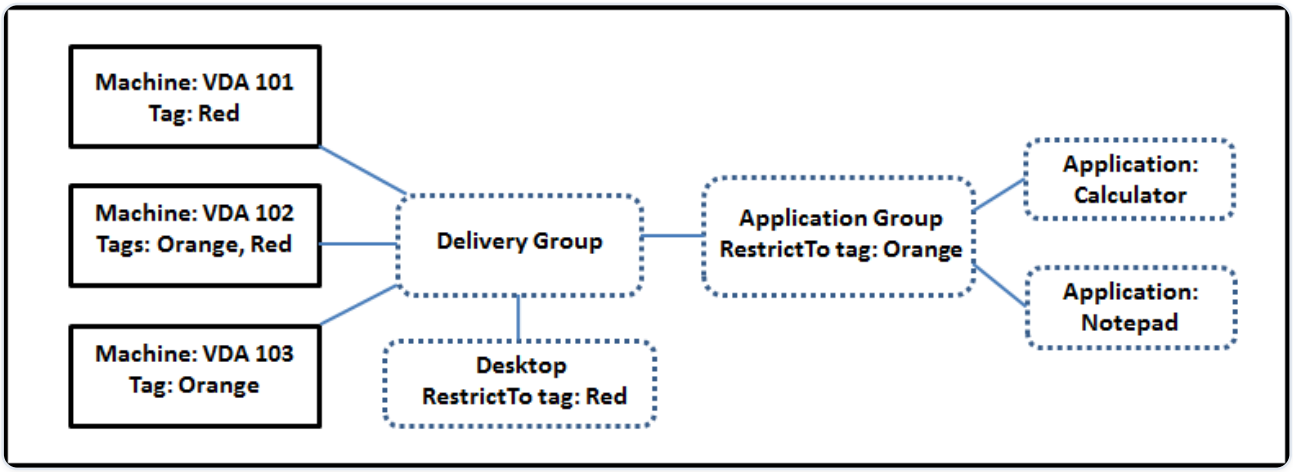

Nesta configuração, os aplicativos são adicionados aos grupos de aplicativos, não aos grupos de entrega. Os grupos de entrega especificam quais máquinas são usadas. (Embora não mostrado, as máquinas estão em catálogos de máquinas.)

O grupo de aplicativos 1 está associado ao grupo de entrega 1. Acesse os aplicativos no grupo de aplicativos 1 pelos usuários especificados no grupo de aplicativos 1. Esses grupos só aparecem enquanto também estiverem na lista de usuários do grupo de entrega 1. Esta configuração segue a orientação de que a lista de usuários para um grupo de aplicativos é um subconjunto (uma restrição) das listas de usuários para os grupos de entrega associados. As configurações no grupo de aplicativos 1 (como compartilhamento de sessão de aplicativo entre grupos de aplicativos, grupos de entrega associados) se aplicam aos aplicativos e usuários nesse grupo. As configurações no grupo de entrega 1 se aplicam aos usuários nos grupos de aplicativos 1 e 2, porque esses grupos de aplicativos foram associados a esse grupo de entrega.

O grupo de aplicativos 2 está associado a dois grupos de entrega: 1 e 2. Cada um desses grupos de entrega recebe uma prioridade no grupo de aplicativos 2, indicando a ordem em que os grupos de entrega são verificados quando um aplicativo é iniciado. Grupos de entrega com prioridade igual são balanceados por carga. Acesse os aplicativos no grupo de aplicativos 2 pelos usuários especificados no grupo de aplicativos 2. No entanto, eles também devem aparecer nas listas de usuários para o grupo de entrega 1 e o grupo de entrega 2.

**Exemplo 2:**

Este layout simples usa restrições de tag para limitar quais máquinas são consideradas para determinados lançamentos de desktop e aplicativos. O site possui um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.




Tags foram adicionadas a cada uma das três máquinas (VDA 101–103).

O grupo de aplicativos foi criado com a restrição de tag "Orange". Cada um de seus aplicativos é iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Orange", VDA 102 e 103.

Para exemplos mais abrangentes e orientações sobre o uso de restrições de tag em grupos de aplicativos (e para desktops), consulte Tags.

## Orientação e considerações

A Citrix recomenda adicionar aplicativos a grupos de aplicativos ou a grupos de entrega, mas não a ambos. Caso contrário, a complexidade adicional de ter aplicativos em dois tipos de grupo pode tornar o gerenciamento mais difícil.

Por padrão, um grupo de aplicativos é habilitado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado. Consulte Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. Este processo requer:

1. Atualizar VDAs nas máquinas usadas no grupo de entrega.
2. Atualizar os catálogos de máquinas que contêm essas máquinas.
3. Atualizar o grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ser no mínimo da versão 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo se refere a "associar" um aplicativo a mais de um grupo de aplicativos. Ele diferencia essa ação de adicionar instâncias desse aplicativo de uma fonte disponível. Da mesma forma, os grupos de entrega são associados a grupos de aplicativos, em vez de serem adições ou componentes uns dos outros.

## Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão de aplicativo está habilitado, todos os aplicativos são iniciados na mesma sessão de aplicativo. Isso economiza os custos associados ao lançamento de mais sessões de aplicativo e permite o uso de recursos de aplicativo que envolvem a área de transferência, como operações de copiar e colar. No entanto, em algumas situações, você pode desativar o compartilhamento de sessão.

Ao usar grupos de aplicativos, você pode configurar o compartilhamento de sessão de aplicativo das três maneiras a seguir, que estendem o comportamento padrão de compartilhamento de sessão disponível ao usar apenas grupos de entrega:

- Compartilhamento de sessão habilitado entre grupos de aplicativos.
- Compartilhamento de sessão habilitado apenas entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desabilitado.

### Compartilhamento de sessão entre grupos de aplicativos

Você pode habilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos ou pode desabilitá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo em que habilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  O grupo de aplicativos 1 contém aplicativos do Microsoft Office, como Word e Excel. O grupo de aplicativos 2 contém outros aplicativos, como Bloco de Notas e Calculadora, e ambos os grupos de aplicativos estão anexados ao mesmo grupo de entrega. Um usuário que tem

acesso a ambos os grupos de aplicativos inicia uma sessão de aplicativo lançando o Word e, em seguida, lançando o Bloco de Notas. Se o controlador descobrir que a sessão existente do usuário executando o Word é adequada para executar o Bloco de Notas, o Bloco de Notas será iniciado dentro da sessão existente. Se o Bloco de Notas não puder ser executado a partir da sessão existente — por exemplo, se a restrição de tag excluir a máquina em que a sessão está sendo executada — então uma nova sessão em uma máquina adequada será criada em vez de usar o compartilhamento de sessão.

- **Um exemplo em que desabilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  Uma configuração com um conjunto de aplicativos que não interoperam bem com outros aplicativos instalados nas mesmas máquinas. Como duas versões diferentes da mesma suíte de software ou duas versões diferentes do mesmo navegador da web. Você prefere não permitir que um usuário inicie ambas as versões na mesma sessão.

  Crie um grupo de aplicativos para cada versão da suíte de software e adicione os aplicativos de cada versão da suíte de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desabilitado para cada um desses grupos de aplicativos, um usuário especificado nesses grupos poderá executar aplicativos da mesma versão na mesma sessão. O usuário ainda pode executar outros aplicativos ao mesmo tempo, mas não na mesma sessão. Ao iniciar um dos aplicativos de versão diferente, ou qualquer aplicativo que não esteja contido em um grupo de aplicativos, esse aplicativo é iniciado em uma nova sessão.

Este recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de sandboxing de segurança. Não é infalível e não pode impedir que os usuários iniciem aplicativos em suas sessões por outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver com capacidade máxima, novas sessões não serão iniciadas nela. Novos aplicativos são iniciados em sessões existentes na máquina conforme necessário, usando o compartilhamento de sessão.

Você só pode disponibilizar sessões pré-iniciadas para grupos de aplicativos que permitem o compartilhamento de sessão de aplicativos. (As sessões que usam o recurso de permanência de sessão estão disponíveis para todos os grupos de aplicativos.) Esses recursos devem ser habilitados e configurados em cada um dos grupos de entrega associados ao grupo de aplicativos. Você não pode configurá-los nos grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Depois de

criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

### Desabilitar o compartilhamento de sessão dentro de um grupo de aplicativos

Você pode impedir o compartilhamento de sessão de aplicativo entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo de quando desabilitar o compartilhamento de sessão dentro de grupos de aplicativos é útil:**

  Você deseja que seus usuários acessem múltiplas sessões simultâneas em tela cheia de um aplicativo em monitores separados.

  Você cria um grupo de aplicativos e adiciona os aplicativos a ele.

Por padrão, o compartilhamento de sessão de aplicativo é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

## Criar um grupo de aplicativos

Para criar um grupo de aplicativos:

1. Faça login no Web Studio.
2. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
3. Para organizar grupos de aplicativos usando pastas, crie pastas sob a pasta raiz **Grupos de Aplicativos**. Para obter mais informações, consulte Organizar grupos de aplicativos usando pastas.
4. Selecione a pasta onde você deseja criar o grupo e clique em **Criar Grupo de Aplicativos**. O assistente de criação de grupo é iniciado com uma página de **Introdução**. Você pode remover a página de futuras inicializações deste assistente.
5. Siga o assistente para configurar as definições nas páginas descritas abaixo. Quando terminar cada página, selecione **Avançar** até chegar à página de **Resumo**.

### Etapa 1. Grupos de Entrega

A página **Grupos de Entrega** lista todos os grupos de entrega, com o número de máquinas que cada grupo contém.

- A lista **Grupos de Entrega Compatíveis** contém grupos de entrega que você pode selecionar. Grupos de entrega compatíveis contêm máquinas de SO de sessão única ou multi-sessão aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Grupos de Entrega Incompatíveis** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como por exemplo, conter máquinas atribuídas estaticamente.

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando o assistente de criação de grupo de aplicativos é confirmado.

Embora você possa criar um grupo de aplicativos que não tenha grupos de entrega associados (talvez para organizar aplicativos ou para servir como armazenamento para aplicativos não utilizados atualmente), o grupo de aplicativos não pode ser usado para entregar aplicativos até que especifique pelo menos um grupo de entrega. Além disso, você não pode adicionar aplicativos ao grupo de aplicativos a partir da fonte do menu **Do Início** se não houver grupos de entrega especificados.

Os grupos de entrega que você seleciona especificam as máquinas que são usadas para entregar aplicativos. Marque as caixas de seleção ao lado dos grupos de entrega que você deseja associar ao grupo de aplicativos.

Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista suspensa.

### Etapa 2. Usuários

Especifique os usuários do aplicativo no grupo de aplicativos. Permita todos os usuários e grupos de usuários nos grupos de entrega que você selecionou na página anterior, ou selecione usuários e grupos de usuários específicos desses grupos de entrega. Se você restringir o uso a usuários especificados, então apenas os usuários especificados no grupo de entrega, o grupo de

aplicativos poderá acessar os aplicativos neste grupo. Essencialmente, a lista de usuários no grupo de aplicativos fornece um filtro nas listas de usuários nos grupos de entrega.

Habilitar ou desabilitar o uso de aplicativos por usuários não autenticados está disponível apenas em grupos de entrega, não em grupos de aplicativos.

Para obter informações sobre onde as listas de usuários são especificadas em uma implantação, consulte Onde as listas de usuários são especificadas.

### Etapa 3. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e já existir um com o mesmo nome nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você concordar com o nome exclusivo sugerido, o aplicativo será adicionado com esse novo nome. Caso contrário, você deve renomeá-lo manualmente antes que possa ser adicionado. Para obter detalhes, consulte Gerenciar pastas de aplicativos.
- Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Consulte Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Nome do aplicativo (para usuário)** no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.
- Quando você adiciona um aplicativo a mais de um grupo de aplicativos, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo foi adicionado.

Clique em **Adicionar** no menu suspenso para exibir as fontes de aplicativos.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta fonte não pode ser selecionada se você selecionou qualquer um dos seguintes:

  - Grupos de aplicativos que não têm grupos de entrega associados.
  - Grupos de aplicativos com grupos de entrega associados que não contêm máquinas.

    - Um grupo de entrega que não contém máquinas.

- **Definido manualmente:** Aplicativos localizados no site ou em outro lugar da sua rede. Ao selecionar esta fonte, uma nova página é aberta onde você digita o caminho para o executável, diretório de trabalho, argumentos opcionais da linha de comando e nomes de exibição para administradores e usuários. Após inserir essas informações, clique em **OK**.
- **Existente**: Aplicativos adicionados anteriormente ao site. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**. Esta fonte não pode ser selecionada se o site não tiver aplicativos.
- **App-V**: Aplicativos em pacotes App-V. Ao selecionar esta fonte, uma nova página é aberta onde você seleciona **Servidor App-V** ou **Biblioteca de Aplicativos**. Na exibição resultante, marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V. Esta fonte não pode ser selecionada (ou pode não aparecer) se o App-V não estiver configurado para o site.

Conforme observado, certas entradas no menu suspenso **Adicionar** não são selecionáveis se não houver uma fonte válida desse tipo. Fontes incompatíveis não são listadas (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos, então essa fonte não é listada ao criar um grupo de aplicativos).

### Etapa 4. Escopos

Esta página aparece somente se você tiver criado anteriormente um escopo personalizado. Por padrão, o escopo **Todos** é selecionado. Para obter mais informações, consulte Administração delegada.

### Etapa 5. Resumo

Insira um nome para o grupo de aplicativos. Você também pode (opcionalmente) inserir uma descrição.

Revise as informações de resumo e clique em **Concluir**.

## Gerenciar grupos de aplicativos

> **Nota:**

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

## Introdução

Este artigo descreve como gerenciar os grupos de aplicativos que você criou.

Consulte Aplicativos para obter informações sobre como gerenciar aplicativos em grupos de aplicativos ou grupos de entrega, incluindo como:

- Adicionar ou remover aplicativos em um grupo de aplicativos.
- Alterar associações de grupo de aplicativos.

O gerenciamento de grupos de aplicativos requer as permissões de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

## Habilitar ou desabilitar um grupo de aplicativos

Quando um grupo de aplicativos está habilitado, ele pode entregar os aplicativos que foram adicionados a ele. Desabilitar um grupo de aplicativos desabilita cada aplicativo nesse grupo. No entanto, se esses aplicativos também estiverem associados a outros grupos de aplicativos habilitados, eles poderão ser entregues a partir desses outros grupos. Se o aplicativo foi explicitamente adicionado a grupos de entrega associados ao grupo de aplicativos, desabilitar o grupo de aplicativos não afeta os aplicativos nesses grupos de entrega.

Um grupo de aplicativos é habilitado quando você o cria. Você não pode alterar essa configuração ao criar o grupo.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, selecione ou desmarque a caixa de seleção **Habilitar Grupo de Aplicativos**.
4. Clique em **Aplicar** para manter a janela aberta ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Habilitar ou desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Para obter mais informações, consulte Compartilhamento de sessão com grupos de aplicativos.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, selecione ou desmarque a caixa de seleção **Habilitar compartilhamento de sessão de aplicativo entre Grupos de Aplicativos**.
4. Clique em **Aplicar** para manter a janela aberta ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Desabilitar o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é habilitado por padrão quando você cria um grupo de aplicativos. Se você desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanecerá habilitado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão de aplicativo desabilitado entre os aplicativos que eles contêm. Em algumas circunstâncias, essa opção é desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não-seamless em janelas de aplicativo de tamanho completo em monitores separados.

Quando você desabilita o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão de aplicativo. Se uma sessão desconectada adequada estiver disponível e executando o mesmo aplicativo, ela será reconectada. Por exemplo, ao iniciar o Bloco de Notas com uma sessão desconectada com o Bloco de Notas em execução, essa sessão é reconectada em vez de criar uma nova. Quando várias sessões desconectadas adequadas estão disponíveis, uma das sessões é escolhida para reconectar, de forma aleatória, mas determinística. Quando a situação se repete nas mesmas circunstâncias, a mesma sessão é escolhida, mas a sessão não é necessariamente previsível de outra forma.

Use o SDK do PowerShell para desabilitar o compartilhamento de sessão de aplicativo para todos os aplicativos em um grupo de aplicativos existente, ou para criar um grupo com o compartilhamento de sessão de aplicativo desabilitado.

### Exemplos de cmdlets do PowerShell

Para desabilitar o compartilhamento de sessão, use os cmdlets do PowerShell do Broker `New-BrokerApplicationGroup` ou `Set-BrokerApplicationGroup` com o parâmetro `SessionSharingEnabled` definido como `False` e o parâmetro `SingleAppPerSession` definido como `True`.

- Por exemplo, para criar um grupo de aplicativos com o compartilhamento de sessão de aplicativo desabilitado para todos os aplicativos no grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Por exemplo, para desabilitar o compartilhamento de sessão de aplicativo entre todos os aplicativos em um grupo de aplicativos existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

### Considerações

- Para habilitar a propriedade `SingleAppPerSession`, você deve definir a propriedade `SessionSharingEnabled` como False. As duas propriedades não devem ser habilitadas ao mesmo tempo. O parâmetro `SessionSharingEnabled` refere-se ao compartilhamento de sessões entre grupos de aplicativos.
- O compartilhamento de sessão de aplicativo funciona apenas para aplicativos associados a grupos de aplicativos, mas não associados a grupos de entrega. Todos os aplicativos associados diretamente a um grupo de entrega compartilham a sessão por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, certifique-se de que os grupos não tenham configurações conflitantes. Por exemplo, um grupo com a opção definida como `True` e a opção de outro grupo definida como `False` resulta em comportamento imprevisível.

## Renomear um grupo de aplicativos

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.

2. Selecione um grupo de aplicativos e, em seguida, selecione **Renomear Grupo de Aplicativos** na barra de ações.
3. Especifique o novo nome exclusivo e, em seguida, clique em **OK**.

## Adicionar, remover ou alterar a prioridade das associações de grupo de entrega com um grupo de aplicativos

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando a caixa de diálogo **Editar Grupo de Aplicativos** é confirmada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.
4. Para adicionar grupos de entrega, clique em **Adicionar**. Selecione as caixas de seleção dos grupos de entrega disponíveis. (Grupos de entrega incompatíveis não podem ser selecionados.) Ao finalizar suas seleções, clique em **OK**.
5. Para remover grupos de entrega, selecione as caixas de seleção dos grupos que deseja remover e, em seguida, clique em **Remover**. Confirme a exclusão quando solicitado.
6. Para alterar a prioridade dos grupos de entrega, selecione a caixa de seleção do grupo de entrega e, em seguida, clique em **Editar Prioridade**. Insira a prioridade (0 = mais alta) e, em seguida, clique em **OK**.
7. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Adicionar, alterar ou remover uma restrição de tag em um grupo de aplicativos

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais máquinas são consideradas para o lançamento de aplicativos. Revise as considerações e advertências em Tags.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.
4. Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista suspensa.
5. Para alterar ou remover uma restrição de tag, selecione uma tag diferente ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com esta tag**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Adicionar ou remover usuários em um grupo de aplicativos

Para obter informações detalhadas sobre usuários, consulte Criar grupos de aplicativos.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Usuários**. Indique se você deseja permitir que todos os usuários nos grupos de entrega associados usem aplicativos no grupo de aplicativos, ou apenas usuários e grupos específicos. Para adicionar usuários, clique em **Adicionar** e, em seguida, especifique os usuários que deseja adicionar. Para remover usuários, selecione um ou mais usuários e, em seguida, clique em **Remover**.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Adicionar, alterar ou remover um ícone de aplicativo em um grupo de aplicativos

Execute as seguintes etapas para adicionar, alterar ou remover um ícone de aplicativo.

1. Selecione **Aplicativos** no painel esquerdo.
2. Na guia **Aplicativos**, selecione um aplicativo e, em seguida, selecione **Propriedades**.

   Para fazer alterações no nível do grupo de aplicativos, navegar até a guia **Grupos de Aplicativos**, selecione um aplicativo em um grupo e, em seguida, selecione **Propriedades**.
3. Selecione a página **Entrega** e, em seguida, selecione **Alterar**. A janela **Selecionar Ícone** é exibida.
4. Na janela **Selecionar Ícone**, faça uma das seguintes ações:

   - Para adicionar um ícone, selecione **Adicionar** e, em seguida, navegue até o ícone.
   - Para remover um ícone, selecione-o e, em seguida, selecione **Remover**.
   - Para alterar um ícone, selecione-o para o aplicativo.

   > **Importante:**
   >
   > - Você não pode adicionar um ícone cujo tamanho seja maior que 200 KB.
   > - Você pode adicionar apenas arquivos .icon.
   > - Você não pode remover ícones incorporados.
   > - Você não pode remover um ícone de um aplicativo que está em uso.

5. Selecione **Salvar** para aplicar as alterações e fechar a janela.

## Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (não é possível editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.

3. Selecione a página **Escopos**. Marque ou desmarque a caixa de seleção ao lado de um escopo.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

## Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (não é possível editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Escopos**. Marque ou desmarque a caixa de seleção ao lado dos escopos que você deseja alterar.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **Salvar** para aplicar as alterações e fechar a janela.

## Excluir um grupo de aplicativos

Um aplicativo deve estar associado a pelo menos um grupo de entrega ou grupo de aplicativos. Se a exclusão de um grupo de aplicativos resultar em um ou mais aplicativos que não pertencem mais a um grupo, você será avisado de que a exclusão desse grupo também removerá esses aplicativos. Você pode então confirmar ou cancelar a exclusão.

A exclusão de um aplicativo não o exclui de sua fonte original. No entanto, se você quiser torná-lo disponível novamente, deverá adicioná-lo novamente.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Excluir Grupo** na barra de ações.
3. Confirme a exclusão quando solicitado.

## Organizar grupos de aplicativos usando pastas

Você pode criar pastas para organizar grupos de aplicativos para facilitar o acesso.

### Funções necessárias

Por padrão, você pode criar e gerenciar pastas para grupos de aplicativos se tiver uma das seguintes funções integradas:

- Administrador da Nuvem
- Administrador Completo
- Administrador de Grupo de Aplicativos

Você pode delegar ações de gerenciamento a outros usuários criando funções personalizadas. A tabela a seguir lista as permissões necessárias para cada ação.

| AÇÃO | PERMISSÕES NECESSÁRIAS |
|---|---|
| Criar pastas de grupo de aplicativos | Criar Pasta de Grupo de Aplicativos |
| Excluir pastas de grupo de aplicativos | Remover Pasta de Grupo de Aplicativos |
| Mover pastas de grupos de aplicativos | Mover Pasta de Grupo de Aplicativos |
| Renomear pastas de grupos de aplicativos | Editar Pasta de Grupo de Aplicativos |
| Mover grupos de aplicativos para pastas | Editar Pasta de Grupo de Aplicativos, Editar Propriedades do Grupo de Aplicativos |

Para obter mais informações, consulte Criar e gerenciar funções.

### Criar e gerenciar pastas

Você pode usar a barra de Ações ou o menu de clique com o botão direito para criar e gerenciar pastas de grupos de aplicativos. Além disso, você pode arrastar um grupo de aplicativos ou uma pasta para um local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas em até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de aplicativos e subpastas. Você só pode excluir uma pasta se ela e suas subpastas não contiverem grupos de aplicativos.
- Todos os nós no Web Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end.

Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Grupos de Aplicativos**, você deve adicionar os metadados `ContainsApplicationGroups` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

Exemplo:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplicationGroups -Value true
```

# Acesso Remoto a PC

**Nota:**

Você pode gerenciar sua implantação de Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente em Citrix Virtual Apps and Desktops 7 2212 ou anterior.

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

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

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

O recurso consiste em um catálogo de máquinas do tipo **Acesso Remoto a PC** que fornece esta funcionalidade:

- Capacidade de adicionar máquinas especificando UOs. Essa capacidade facilita a adição de PCs em massa.
- Atribuição automática de usuário com base no usuário que faz login no PC Windows do escritório. Suportamos atribuições de usuário único e múltiplos usuários. Por padrão, atribuímos automaticamente múltiplos usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, faça login no Web Studio, vá para **Configurações** e desative a configuração **Habilitar atribuição automática de múltiplos usuários para Acesso Remoto a PC**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs Linux Físicos
- PCs físicos agrupados (ou seja, atribuídos aleatoriamente, não dedicados)

> **Notas:**

> Para obter detalhes sobre as versões de SO suportadas, consulte os requisitos de sistema para o VDA para SO de sessão única e VDA Linux.

> Para implantações locais, o Acesso Remoto a PC é válido apenas para licenças Citrix Virtual Apps and Desktops Advanced ou Premium. As sessões consomem licenças da mesma forma que outras sessões do Citrix Virtual Desktops™. Para o Citrix Cloud, o Acesso Remoto a PC é válido para Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) e Workspace Premium Plus.

## Considerações

Embora todos os requisitos técnicos e considerações que se aplicam ao Citrix Virtual Apps and Desktops em geral também se apliquem ao Acesso Remoto a PC, alguns podem ser mais relevantes ou exclusivos para o caso de uso de PC físico.

**Importante:**

Sistemas físicos com Windows 11 (e alguns executando Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:

- Use a opção "/physicalmachine" juntamente com a opção "/remotepc" como parte da instalação do VDA por linha de comando
- Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada não tenha sido usada `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - Nome: ForceEnableRemotePC
  - Tipo: DWORD
  - Dados: 1

## Considerações de implantação

Ao planejar a implantação do Acesso Remoto a PC, tome algumas decisões gerais.

- Você pode adicionar o Acesso Remoto a PC a uma implantação existente do Citrix Virtual Apps and Desktops. Antes de escolher esta opção, considere o seguinte:
  - Os Delivery Controllers ou Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os bancos de dados do site on-premises e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os VDAs existentes e os novos VDAs de Acesso Remoto a PC excederão o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs de escritório por meio de um processo automatizado. As seguintes são as opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instalar VDAs usando SCCM.
  - Scripts de implantação: Instalar VDAs usando scripts.

- Revise as considerações de segurança do Acesso Remoto a PC.

> **Observação:**
>
> Ao projetar o Acesso Remoto a PC, você deve considerar o número de monitores físicos conectados à GPU no PC remoto e atualmente configurados/operando. Mesmo que o monitor não seja usado na sessão Citrix, mas seja detectado pela GPU, a presença do monitor é contabilizada para o limite máximo de monitores suportados pela GPU.

## Considerações sobre o catálogo de máquinas

O tipo de catálogo de máquinas necessário depende do caso de uso:

- Catálogo de máquinas de Acesso Remoto a PC
  - PCs Windows dedicados
  - PCs Windows dedicados multiusuário. Este caso de uso se aplica a PCs físicos de escritório que múltiplos usuários podem acessar remotamente em diferentes turnos.
  - PCs Windows agrupados. Este caso de uso se aplica a PCs físicos que múltiplos usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas de SO de sessão única
  - Estático - PCs Linux dedicados
  - Aleatório - PCs Linux Agrupados

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.
- Ao escolher as UOs nas quais as contas de máquina residem, selecione UOs de nível inferior para maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de Banco/Oficiais/Caixas, selecione **Caixas** para maior granularidade. Caso contrário, você pode selecionar **Oficiais** ou **Banco** com base no requisito.
- Mover ou excluir UOs depois de serem atribuídas a um catálogo de máquinas de Acesso Remoto a PC afeta as associações de VDA e causa problemas com atribuições futuras.

Portanto, certifique-se de planejar adequadamente para que as atualizações de atribuição de UO para catálogos de máquinas sejam consideradas no plano de alteração do Active Directory.

- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas devido à estrutura da UO, você não precisa selecionar nenhuma UO. Você pode usar o PowerShell para adicionar máquinas ao catálogo posteriormente. As atribuições automáticas de usuário continuam a funcionar se a atribuição de desktop estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo de máquinas juntamente com as atribuições de usuário está disponível no GitHub.
- O Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Acesso Remoto a PC**.

## Considerações sobre o VDA Linux

Estas considerações são específicas para o VDA Linux:

- Use o VDA Linux em máquinas físicas apenas no modo não 3D. Devido a limitações no driver da NVIDIA, a tela local do PC não pode ser escurecida e exibe as atividades da sessão quando o modo HDX 3D está ativado. Exibir esta tela é um risco de segurança.
- Use catálogos de máquinas do tipo SO de sessão única para máquinas Linux físicas.
- A atribuição automática de usuário não está disponível para máquinas Linux.
- Se os usuários já estiverem logados em seus PCs localmente, as tentativas de iniciar os PCs a partir do StoreFront™ falharão.
- As opções de economia de energia não estão disponíveis para máquinas Linux.

## Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e considerações para PCs físicos.

- O seguinte não é suportado:
  - Comutadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo laptops e PCs All-in-One e NVIDIA Optimus.
  - Máquinas com dual boot.
- Conecte o teclado e o mouse diretamente ao PC. A conexão a um monitor ou outros componentes que podem ser desligados ou desconectados pode tornar esses periféricos indisponíveis. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desligue esses componentes.

- Os PCs devem estar ingressados em um domínio do Active Directory Domain Services.
- O Secure Boot é suportado apenas no Windows 10 e Windows 11.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é preferível para maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:

  a. Defina as configurações de energia para manter o adaptador sem fio ligado.

  b. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registrará até que o usuário faça logon. O PC não estará disponível para acesso remoto até que um usuário tenha feito logon.

  c. Certifique-se de que os Delivery Controllers ou Cloud Connectors possam ser alcançados a partir da rede Wi-Fi.

- Você pode usar o Acesso Remoto ao PC em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionar com a bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:

  a. Desative o recurso de hibernação.

  b. Desative o recurso de suspensão.

  c. Defina a ação de fechar a tampa como **Não fazer nada**.

  d. Defina a ação de "pressionar o botão liga/desliga" como **Desligar**.

  e. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Acesso Remoto ao PC é compatível com dispositivos Surface Pro com Windows 10. Siga as mesmas diretrizes para laptops mencionadas anteriormente.
- Se estiver usando uma estação de acoplamento, você pode desacoplar e reacoplar laptops. Ao desacoplar o laptop, o VDA se registra novamente com os Delivery Controllers ou Cloud Connectors via Wi-Fi. No entanto, ao reacoplar o laptop, o VDA não muda para usar a conexão com fio, a menos que você desconecte o adaptador sem fio. Alguns dispositivos fornecem funcionalidade integrada para desconectar o adaptador sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador sem fio. Revise as considerações sobre Wi-Fi mencionadas anteriormente.

  Faça o seguinte para habilitar o acoplamento e desacoplamento para dispositivos de Acesso Remoto ao PC:

a. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão** e defina **Suspender** como **Nunca**.

b. Em **Gerenciador de Dispositivos > Adaptadores de rede > Adaptador Ethernet**, vá para **Gerenciamento de Energia** e desmarque **Permitir que o computador desligue este dispositivo para economizar energia**. Certifique-se de que **Permitir que este dispositivo reative o computador** esteja marcado.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, esse recurso aparece como indisponível se já estiver em uso por outro usuário.
- Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

## Sequência de configuração

Esta seção contém uma visão geral de como configurar o Acesso Remoto ao PC ao usar o catálogo de máquinas do tipo **Acesso Remoto ao PC**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquinas.

1. Somente site local - Para usar o recurso integrado Wake on LAN, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para Acesso Remoto ao PC:

   a. Selecione o tipo de Site **Acesso Remoto a PC**.

   b. Na página **Gerenciamento de Energia**, escolha habilitar ou desabilitar o gerenciamento de energia para o catálogo de máquinas padrão de Acesso Remoto ao PC. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.

   c. Preencha as informações nas páginas **Usuários** e **Contas de Máquina**.

   A conclusão dessas etapas cria um catálogo de máquinas chamado **Máquinas de Acesso Remoto a PC** e um Grupo de Entrega chamado **Desktops de Acesso Remoto a PC**.
3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a. Crie um catálogo de máquinas do tipo **Acesso Remoto ao PC** (página Sistema Operacional do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Certifique-se de atribuir a OU correta para que os PCs de destino fiquem disponíveis para uso com o Acesso Remoto ao PC.

b. Crie um Grupo de Entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um Grupo de Entrega, consulte Criar Grupos de Entrega. Certifique-se de atribuir o Grupo de Entrega a um grupo do Active Directory que contenha os usuários que precisam de acesso aos seus PCs.

4. Implante o VDA nos PCs do escritório.

   - Recomendamos usar o instalador VDA principal do SO de sessão única (VDAWorkstationCoreSetup.exe).
   - Você também pode usar o instalador VDA completo de sessão única (VDAWorkstationSetup.exe) com a opção `/remotepc/physicalmachine`, que alcança o mesmo resultado que usar o instalador VDA principal.

     > **Observação:**
     >
     > Para a instalação do RemotePC, use o argumento `/physicalmachine` com `/remotepc` para que o VDA se comporte conforme o esperado em certos cenários de usuário.

   - Considere habilitar a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto através do Citrix Director. Para fazer isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para poder ver as informações de duração de logon no Director, você deve usar o instalador VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Inclua este componente usando a opção `/includeadditional`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para obter informações sobre como implantar o VDA usando o SCCM, consulte Instalar VDAs usando o SCCM.
   - Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

   Depois de concluir com sucesso as etapas 2 a 4, os usuários são automaticamente atribuídos às suas próprias máquinas quando fazem login localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente que eles usam para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace

está disponível em `https://www.citrix.com/downloads/` ou nas lojas de aplicativos para dispositivos móveis compatíveis.

## Recursos gerenciados através do registro

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

### Desabilitar atribuições automáticas de múltiplos usuários

Em cada Delivery Controller™, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dados: 0

### Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina de Acesso Remoto a PC entre em estado de suspensão, adicione esta configuração de registro no VDA e, em seguida, reinicie a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra em modo de suspensão após o tempo limite de inatividade pré-configurado. Depois que a máquina acorda, ela se registra novamente com o Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Valor: 1

### Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é automaticamente desconectada quando um usuário local inicia uma sessão nessa máquina (pressionando CTRL+ATL+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e, em seguida, reinicie a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Valor: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é reconhecida dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Valor:
  - 1 - O usuário remoto sempre tem preferência se ele ou ela não responder à interface de mensagens no período de tempo limite especificado. Este comportamento é o padrão se esta configuração não for definida.
  - 2 - O usuário local tem preferência.

O tempo limite para aplicar o modo Acesso Remoto ao PC é de 30 segundos por padrão. Você pode configurar esse tempo limite, mas não o defina para menos de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dados: número de segundos para o tempo limite em valores decimais

Quando um usuário deseja obter acesso forçado ao console: O usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local sobre uma sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon nesse PC enquanto ele estiver em uso por um usuário remoto, o usuário remoto receberá um prompt. O prompt pergunta se deve permitir ou negar a conexão do usuário local. Permitir a conexão desconecta a sessão do usuário remoto.

## Registro de gerenciamento de sessão

O Acesso Remoto ao PC agora possui recursos de registro que registram quando alguém tenta acessar um PC com uma sessão ICA® ativa. Isso permite que você monitore seu ambiente em busca de atividades indesejadas ou inesperadas e seja capaz de auditar esses eventos, caso precise investigar quaisquer incidentes.

Os eventos são registrados usando o Visualizador de Eventos do Windows e estão em **Aplicativos e Serviços > Citrix > HostCore > ICA Service > Admin**.

Existem três eventos distintos que são registrados ao usar o Acesso Remoto ao PC.

### Evento Ctrl+Alt+Del

Este evento aparece quando o usuário local pressiona Ctrl+Alt+Del no teclado do console com uma sessão remota ativa.

#### Detalhes do evento

- Nome do log: Aplicativo e Serviços
- ID do evento: 43, 44, 45
- Fonte: ICA Service

#### ID do Evento 43

Este ID de evento aparece quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

#### ID do Evento 44

Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The user preference is set to remote user.
```

#### ID do Evento 45

Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

### Evento de desconexão de sessão remota

Este evento aparece quando a sessão remota foi desconectada por vários motivos.

### Detalhes do evento

- Nome do log: Aplicativo e Serviços
- ID do Evento: 46, 47, 48
- Fonte: ICA Service

#### ID do Evento 46

Este ID de evento aparece quando a sessão remota foi desconectada e quando o valor do registro SasNotification não existe ou o valor do registro SasNotification é 0.

- Mensagem:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

### ID do Evento 47

Este ID de evento aparece quando o usuário remoto concorda em desconectar a sessão e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode é 2 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

### ID do Evento 48

Este ID de evento aparece quando o usuário remoto não recusa a solicitação de desconexão dentro do período de tempo limite específico e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

### Evento de pressionar Ctrl+Alt+Del duas vezes

Este evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

### Detalhes do evento

- Nome do log: Aplicativos e Serviços
- 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:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

# Wake on LAN

O Acesso Remoto ao PC suporta Wake on LAN, o que oferece aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs de escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina foi desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede na qual o PC reside quando instruído pelo delivery controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura extras ou soluções de terceiros para a entrega de pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN baseado em SCCM legado. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN – SCCM-integrated.

## Limitação

O Acesso Remoto ao PC com o recurso Wake on LAN não suporta o ligamento automático durante os horários de pico.

## Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes de compatibilidade, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows

## Configurar Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops no local, a configuração do Wake on LAN integrado é suportada apenas usando PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas do Acesso Remoto ao PC se você ainda não tiver um.
2. Crie a conexão de host do Wake on LAN se você ainda não tiver uma.

> **Observação:**
>
> Para usar o recurso Wake on LAN, se você tiver uma conexão de host do tipo "Microsoft Configuration Manager Wake on LAN", crie uma nova conexão de host.

3. Recupere o identificador exclusivo da conexão de host do Wake on LAN.
4. Associe a conexão de host do Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host Wake on LAN:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `
```

```
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties>"
`
                -Persist


$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid


# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
}
```

Quando a conexão de host estiver pronta, execute os seguintes comandos para recuperar o identificador exclusivo da conexão de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
```

Depois de recuperar o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo de máquinas do Acesso Remoto ao PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

### Considerações de design

Ao planejar usar o Wake on LAN com o Acesso Remoto ao PC, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host do Wake on LAN.
- Para que um PC ative outro PC, ambos os PCs devem estar na mesma sub-rede e usar a mesma conexão de host do Wake on LAN. Não importa se os PCs estão no mesmo catálogo de máquinas ou em catálogos diferentes.
- As conexões de host são atribuídas a zonas específicas. Se sua implantação contiver mais de uma zona, você precisará de uma conexão de host do Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Pacotes mágicos são transmitidos usando o endereço de broadcast global 255.255.255.255. Certifique-se de que o endereço não esteja bloqueado.
- Deve haver pelo menos um PC ligado na sub-rede — para cada conexão Wake on LAN — para poder ativar máquinas nessa sub-rede.

### Considerações operacionais

A seguir estão as considerações para usar o recurso Wake on LAN:

- O VDA deve se registrar pelo menos uma vez antes que o PC possa ser ativado usando o recurso integrado Wake on LAN.
- O Wake on LAN só pode ser usado para ativar PCs. Ele não oferece suporte a outras ações de energia, como reiniciar ou desligar.
- Depois que a conexão Wake on LAN é criada, ela fica visível no Web Studio. No entanto, a edição de suas propriedades no Web Studio não é suportada se estiver usando o Citrix Virtual Apps and Desktops no local.
- Pacotes mágicos são enviados de uma das duas maneiras:

  a. Quando um usuário tenta iniciar uma sessão em seu PC e o VDA está não registrado

  b. Quando um administrador envia manualmente um comando de ligar do Web Studio ou PowerShell

- Como o delivery controller não tem conhecimento do estado de energia de um PC, o Web Studio exibe **Não Suportado** em estado de energia. O delivery controller usa o estado de registro do VDA para determinar se um PC está ligado ou desligado.

# Wake on LAN – Integrado ao SCCM

O Wake on LAN integrado ao SCCM é uma opção alternativa de Wake on LAN para Acesso Remoto a PC que está disponível apenas com o Citrix Virtual Apps and Desktops no local.

## Requisitos do sistema

A seguir estão os requisitos de sistema para usar o recurso Wake on LAN integrado ao SCCM:

- Citrix Virtual Apps and Desktops 1912 ou posterior
- PCs físicos:
  - VDA versão 1912 ou posterior
  - Windows 10. Para obter detalhes de compatibilidade, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou posterior

## Configurar Wake on LAN integrado ao 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 Acesso Remoto a PC, dando tempo para que o ciclo de inventário agendado do SCCM seja executado, ou force um manualmente, se necessário.
2. Para suporte a Wake Proxy, habilite a opção no SCCM. Para cada sub-rede na organização que contém PCs que usam o recurso Wake on LAN de Acesso Remoto a PC, certifique-se de que três ou mais máquinas possam servir como máquinas sentinela.
3. Para suporte a pacotes mágicos, configure roteadores de rede e firewalls para permitir que pacotes mágicos sejam enviados, usando uma transmissão direcionada à sub-rede ou unicast.
4. Configure o Wake on LAN nas configurações de BIOS/UEFI de cada PC.
5. Implante o VDA nos PCs físicos, se ainda não o fez.

Depois de atender aos pré-requisitos, conclua as seguintes etapas para permitir que o Delivery Controller se comunique com o SCCM:

1. Crie uma conexão de host para o SCCM. Para obter mais informações, consulte Conexões e recursos.

- Selecione **Microsoft Configuration Manager Wake on LAN** como o tipo de conexão.
- As credenciais inseridas devem ter acesso às coleções no escopo e devem ter a função de **Operador de Ferramentas Remotas**.

2. Selecione a conexão no Web Studio, depois selecione **Editar Conexão**, e clique em **Avançado**.
3. Selecione a opção apropriada para lidar com o Wake on LAN:

    - Se você estiver usando o proxy de ativação, selecione a primeira opção: **Proxy de ativação do Microsoft System Center Configuration Manager**.
    - Se você estiver usando pacotes mágicos, selecione a segunda opção: **Pacotes Wake on LAN transmitidos pelo Delivery Controller**.
        - Selecione o método de transmissão apropriado: **transmissões direcionadas por sub-rede** ou **unicast**.

Depois de criar a conexão do host, associe a conexão a um catálogo de Acesso Remoto para PC:

- Se você estiver criando um novo catálogo de Acesso Remoto para PC, na página **Sistema Operacional** do assistente de criação de catálogo, selecione **Acesso Remoto para PC** como o tipo de catálogo e escolha a conexão apropriada na lista suspensa.
- Para adicionar o Wake on LAN a um catálogo de Acesso Remoto para PC existente:

    a. Vá para o nó **Catálogos de Máquinas** no Web Studio, selecione o catálogo de máquinas e, em seguida, selecione **Editar Catálogo de Máquinas**.

    b. Selecione a guia **Gerenciamento de Energia** e escolha **Sim** para habilitar o gerenciamento de energia para o catálogo de máquinas.

    c. Selecione a conexão apropriada na lista suspensa e clique em **OK**.

## Solução de problemas

### Escurecimento do monitor não funciona

Se o monitor local do PC Windows não estiver em branco durante uma sessão HDX ativa (o monitor local exibe o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê ao driver de exibição indireta (IDD) da Citrix uma prioridade maior do que o driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para mais detalhes sobre as prioridades do adaptador de vídeo e a criação de monitores, consulte o artigo do Knowledge Center CTX237608.

### A sessão se desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão habilitada

A notificação de gerenciamento de sessão controlada pelo valor de registro **SasNotification** só funciona quando o modo Acesso Remoto para PC está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização habilitados, o PC será relatado como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desabilitará automaticamente o modo Acesso Remoto para PC. Para habilitar o modo Acesso Remoto para PC, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

### Informações de diagnóstico

As informações de diagnóstico sobre o Acesso Remoto para PC são gravadas no log de Eventos de Aplicativo do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas descartando mensagens duplicadas.

- 3300 (informativo): Máquina adicionada ao catálogo
- 3301 (informativo): Máquina adicionada ao grupo de entrega
- 3302 (informativo): Máquina atribuída ao usuário
- 3303 (erro): Exceção

### Gerenciamento de energia

Se o gerenciamento de energia para Acesso Remoto para PC estiver habilitado, as transmissões direcionadas por sub-rede podem falhar ao iniciar máquinas que estão em uma sub-rede diferente do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando

transmissões direcionadas por sub-rede, e o suporte AMT não estiver disponível, tente o proxy de ativação ou o método Unicast. Certifique-se de que essas configurações estejam habilitadas nas propriedades avançadas para a conexão de gerenciamento de energia.

### A sessão remota ativa registra a entrada local da tela de toque

Quando o VDA ativa o modo de Acesso Remoto ao PC, a máquina ignora a entrada local da tela de toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização ativados, o PC se reporta como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo de Acesso Remoto ao PC. Para ativar o modo de Acesso Remoto ao PC, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

## Mais recursos

A seguir estão outros recursos para Acesso Remoto ao PC:

- Orientação de design da solução: Remote PC Access Design Decisions.
- Exemplos de arquiteturas de Acesso Remoto ao PC: Reference Architecture for Citrix Remote PC Access Solution.

# Publicar conteúdo

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

> Você pode publicar um aplicativo que é simplesmente um URL ou caminho UNC para um recurso, como um documento do Microsoft Word ou um link da web. Esse recurso é conhecido como conteúdo publicado. A capacidade de publicar conteúdo adiciona flexibilidade à forma como você entrega conteúdo aos usuários. Você se beneficia do controle de acesso e gerenciamento de aplicativos existentes. Você também pode especificar se deseja usar aplicativos locais ou publicados para abrir o conteúdo.

O conteúdo publicado aparece como outros aplicativos no StoreFront™ e no aplicativo Citrix Workspace™. Os usuários o acessam da mesma forma que acessam os aplicativos. No cliente, o recurso é aberto normalmente.

- Se um aplicativo instalado localmente for apropriado, ele será iniciado para abrir o recurso.
- Se uma Associação de Tipo de Arquivo tiver sido definida, um aplicativo publicado será iniciado para abrir o recurso.

Você publica conteúdo usando o SDK do PowerShell. Você não pode usar o Web Studio para publicar conteúdo. No entanto, você pode usar o Web Studio para editar as propriedades do aplicativo posteriormente, depois que forem publicados.

## Visão geral e preparação da configuração

A publicação de conteúdo usa o cmdlet `New-BrokerApplication` com as seguintes propriedades principais. (Consulte a ajuda do cmdlet para descrições de todas as propriedades do cmdlet.)

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

A propriedade `ApplicationType` deve ser `PublishedContent`.

A propriedade `CommandLineExecutable` especifica o local do conteúdo publicado. Os seguintes formatos são suportados, com um limite de 255 caracteres.

- Endereço de site HTML (por exemplo, `<http://www.citrix.com>`)
- Arquivo de documento em um servidor web (por exemplo, `https://www.citrix.com/press/pressrelease.doc`)
- Diretório em um servidor FTP (por exemplo, `ftp://ftp.citrix.com/code`)

- Arquivo de documento em um servidor FTP (por exemplo, `ftp://ftp.citrix.com/code/Readme.txt`>)
- Caminho de diretório UNC (por exemplo, `file://myServer/myShare or \\\\myServer\\myShare`)
- Caminho de arquivo UNC (por exemplo, `file://myServer/myShare/myFile.asf` ou `\\myServer\myShare\myFile.asf`)

Certifique-se de que você tenha o SDK correto.

- Para implantações do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), baixe e instale o SDK remoto do PowerShell do Citrix Virtual Apps and Desktops.
- Para implantações locais do Citrix Virtual Apps and Desktops, use o SDK do PowerShell que é instalado com o Delivery Controller. Adicionar um aplicativo de conteúdo publicado requer um Delivery Controller de versão mínima 7.11.

Os procedimentos a seguir usam exemplos. Nos exemplos:

- Um catálogo de máquinas foi criado.
- Um grupo de entrega chamado `PublishedContentApps` foi criado. O grupo usa uma máquina de SO multi-sessão do catálogo. O aplicativo WordPad foi adicionado ao grupo.
- As atribuições são feitas para o nome do grupo de entrega, o local `CommandLineExecutable` e o nome do aplicativo.

## Começar

Na máquina que contém o SDK do PowerShell, abra o PowerShell.

O cmdlet a seguir adiciona o snap-in apropriado do SDK do PowerShell e atribui o registro do grupo de entrega retornado.

```
Add-PsSnapin Citrix&ast; $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Se você estiver usando o Citrix DaaS, autenticar inserindo suas credenciais do Citrix Cloud™. Se houver mais de um cliente, escolha um.

### Publicar uma URL

Depois de atribuir o local e o nome do aplicativo, o cmdlet a seguir publica a página inicial da Citrix como um aplicativo.

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

Verificar sucesso:

- Abra o StoreFront e faça logon como um usuário que pode acessar aplicativos no grupo de entrega PublishedContentApps. A exibição inclui o aplicativo recém-criado com o ícone padrão. Para saber mais sobre como personalizar o ícone, consulte `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`.
- Clique no aplicativo **Citrix Home Page**. A URL é iniciada em uma nova guia em uma instância local do seu navegador padrão.

## Publicar recursos localizados em caminhos UNC

Neste exemplo, o administrador já criou um compartilhamento chamado `PublishedResources`. Depois de atribuir os locais e os nomes dos aplicativos, os seguintes cmdlets publicam um arquivo RTF e um DOCX nesse compartilhamento como um recurso.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
```

```
$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

Verificar o sucesso:

- Atualize sua janela do StoreFront para ver os documentos recém-publicados.
- Clique nos aplicativos **PublishedRTF** e **PublishedDOCX**. Cada documento é aberto em um WordPad em execução localmente.

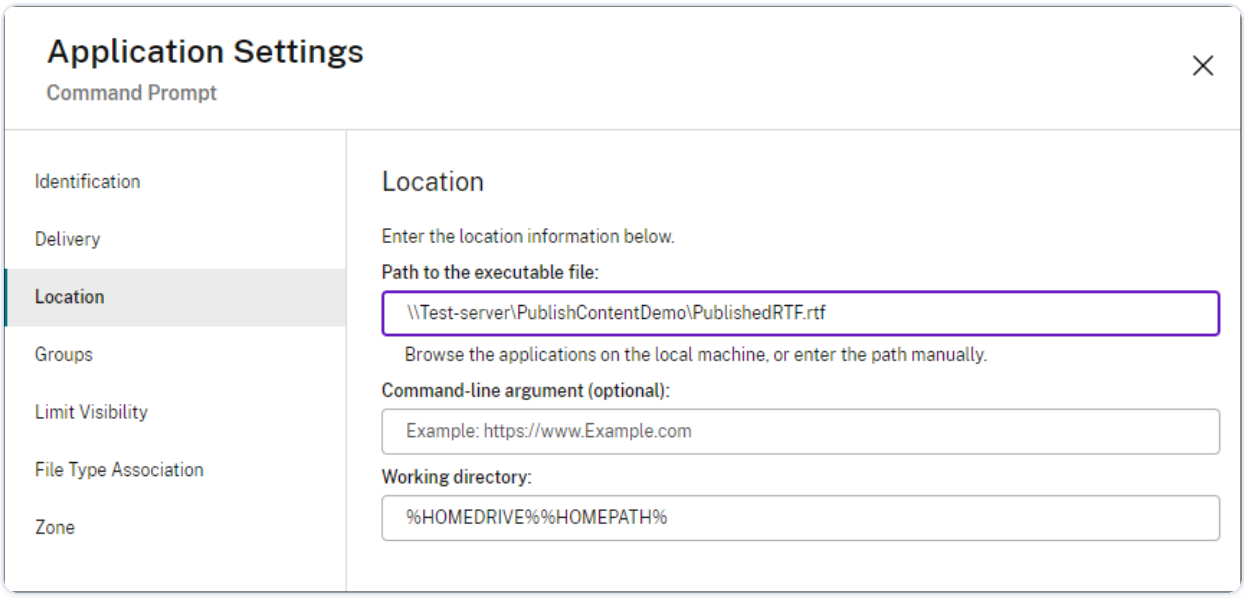
## Visualizar e editar aplicativos PublishedContent

Você gerencia o conteúdo publicado usando os mesmos métodos que usa para outros tipos de aplicativos.

Para visualizar e editar aplicativos `PublishedContent`, siga estas etapas:

1. Faça logon no Web Studio e selecione **Aplicativos** no painel esquerdo.
2. Na guia **Aplicativos**, selecione um aplicativo PublishedContent e, em seguida, selecione **Propriedades**.

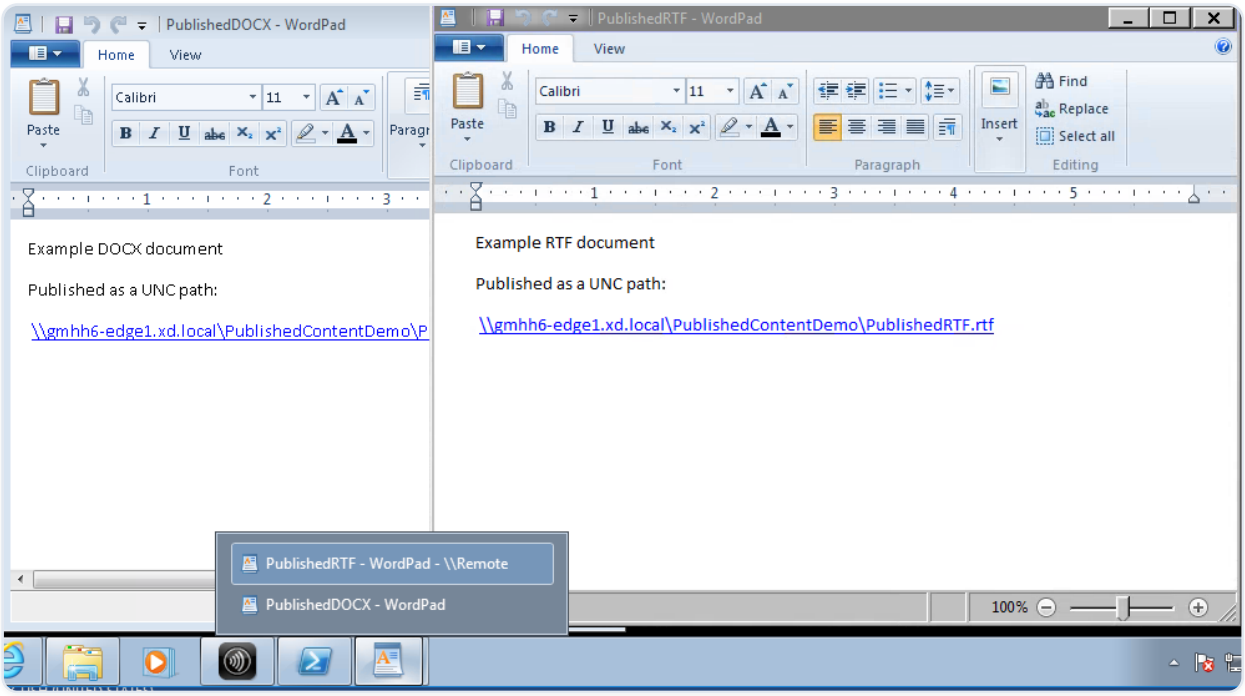
   As propriedades do aplicativo (como visibilidade do usuário, associação de grupo e atalho) se aplicam ao conteúdo publicado. No entanto, você não pode alterar o argumento da linha de comando ou as propriedades do diretório de trabalho na página **Local**.
3. Para alterar o recurso, modifique o campo **Caminho para o arquivo executável** nessa página.




4. Para usar um aplicativo publicado para abrir um aplicativo `PublishedContent` (em vez de um aplicativo local), siga estas etapas:

   Neste exemplo, o aplicativo WordPad publicado é editado para criar uma Associação de Tipo de Arquivo para arquivos .rtf.

   a. Ative o modo de manutenção para o grupo de entrega.
   b. Edite a propriedade **Associação de Tipo de Arquivo**.
   c. Desative o modo de manutenção quando terminar.
   d. Atualize o StoreFront para carregar as alterações da Associação de Tipo de Arquivo e, em seguida, clique nos aplicativos **PublishedRTF** e **PublishedDOCX**. Observe a diferença. **PublishedDOCX** ainda abre no WordPad local. No entanto, **PublishedRTF** agora abre no WordPad publicado devido à associação de tipo de arquivo.




## Para mais informações

- Criar catálogos de máquinas
- Criar grupos de entrega
- Alterar propriedades do aplicativo

# Server VDI

Use o recurso Server VDI (Virtual Desktop Infrastructure) para entregar um desktop de um sistema operacional de servidor para um único usuário.

- Administradores corporativos podem entregar sistemas operacionais de servidor como desktops VDI, o que pode ser valioso para usuários como engenheiros e designers.
- Provedores de Serviço podem oferecer desktops da nuvem. Esses desktops estão em conformidade com o Contrato de Licença de Provedor de Serviços da Microsoft (SPLA).

Suporte:

- Em implantações de Citrix Virtual Apps and Desktops™ e Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), o Server VDI é suportado no Windows Server 2022, Windows Server 2019 e Windows Server 2016.
- Todas as implantações de Server VDI suportam a tecnologia de camada de personalização do usuário.

- Para que o Server VDI funcione com dispositivos TWAIN, como scanners, o recurso Experiência de Área de Trabalho do Windows Server deve ser instalado.
- Os seguintes recursos não podem ser usados com o Server VDI:
  - Aplicativos hospedados
  - Acesso a Aplicativos Locais
  - Conexões de desktop diretas (não intermediadas)
  - Acesso Remoto ao PC

## Instalar e configurar o Server VDI

1. Prepare o servidor Windows para a instalação.
   - Use o Gerenciador do Servidor Windows para garantir que os serviços de função dos Serviços de Área de Trabalho Remota não estejam instalados. Se eles foram instalados anteriormente, remova-os. A instalação do VDA falha se esses serviços de função estiverem instalados.
   - Certifique-se de que a propriedade **Restringir cada usuário a uma única sessão** esteja habilitada. No servidor Windows, edite o registro para a configuração do Terminal Server:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Use a interface de linha de comando do instalador do Citrix Virtual Apps and Desktops para instalar um VDA em um servidor compatível ou imagem mestra de servidor, especificando a opção `/servervdi`. (Por padrão, a interface gráfica do instalador bloqueia o VDA de SO de sessão única do Windows em um sistema operacional de servidor. O uso da linha de comando substitui esse comportamento.) Use um dos seguintes comandos:
   - Implantações do Citrix Virtual Apps and Desktops:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Implantações do Citrix DaaS™:
     - `VDAWorkstationSetup.exe /servervdi`

   Outras opções:

- Use `/controllers` para especificar Delivery Controllers ou Cloud Connectors.
- Use `/enable_hdx_ports` para abrir portas no firewall, a menos que o firewall seja configurado manualmente.
- Use `/mastermcsimage` (ou `/masterimage`) se estiver instalando o VDA em uma imagem e for usar o MCS para criar VMs de servidor a partir dessa imagem.
- Para todos os detalhes das opções, consulte Instalar usando a linha de comando.

3. Crie um catálogo de máquinas para Server VDI. No assistente de criação de catálogo:
   - Na página **Sistema Operacional**, selecione **SO de sessão única**.
   - Na página **Resumo**, especifique um nome de catálogo de máquinas e uma descrição para administradores que o identifique claramente como Server VDI. Este é o único indicador no Studio de que o catálogo oferece suporte a Server VDI.

   Ao usar a pesquisa no Studio, o catálogo Server VDI é exibido na guia **Máquinas de SO de sessão única**, mesmo que o VDA esteja instalado em uma máquina multi-sessão.
4. Crie um Grupo de Entrega e selecione o catálogo Server VDI que você criou.

Se você não especificou Delivery Controllers ou Cloud Connectors durante a instalação do VDA, lembre-se de especificá-los depois. Para obter detalhes, consulte Registro do VDA.

# Camada de personalização do usuário

> **Nota:**

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

> O recurso de camada de personalização do usuário para Citrix Virtual Apps and Desktops estende os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e os aplicativos instalados localmente entre as sessões. Alimentado pela tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e ao Machine Creation Services™ (MCS) em um catálogo de máquinas não persistente.

Você instala os componentes da camada de personalização do usuário junto com o Virtual Delivery Agent dentro da imagem mestre. Um arquivo VHD armazena aplicativos instalados localmente pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

> **Importante:**
>
> Você pode implantar camadas de personalização do usuário no Citrix Virtual Apps and Desktops, ou camadas de usuário do App Layering habilitadas em um modelo de imagem, não ambos. Não instale o recurso de camada de personalização do usuário em uma camada dentro do App Layering.

> Este recurso substitui o Personal vDisk (PvD), ao mesmo tempo em que oferece uma experiência de espaço de trabalho persistente para usuários em um ambiente de desktop não persistente (agrupado).

Para implantar o recurso de camada de personalização do usuário, instale e configure-o usando as etapas detalhadas no artigo.

## Suporte a aplicativos

Com exceção das seguintes, todos os aplicativos que um usuário instala localmente na área de trabalho são suportados na camada de personalização do usuário.

### Exceções

Os seguintes aplicativos são exceção e não são suportados na camada de personalização do usuário:

- Aplicativos corporativos, como MS Office e Visual Studio.
- Aplicativos que modificam a pilha de rede ou o hardware. Exemplo: um cliente VPN.
- Aplicativos que possuem drivers de nível de inicialização. Exemplo: um antivírus.
- Aplicativos com drivers que usam o armazenamento de drivers. Exemplo: um driver de impressora.

> **Nota:**

> Você pode disponibilizar impressoras usando Objetos de Política de Grupo (GPOs) do Windows.

Não *permita* que os usuários instalem aplicativos não suportados localmente. Em vez disso, instale esses aplicativos diretamente na imagem mestre.

### Aplicativos que exigem uma conta de usuário local ou de administrador

Quando um usuário instala um aplicativo localmente, o aplicativo vai para a sua camada de usuário. Se o usuário adicionar ou editar um usuário ou grupo local, as alterações não persistem além da sessão.

> **Importante:**
>
> Adicione qualquer usuário ou grupo local necessário na imagem mestre.

## Requisitos

O recurso de camada de personalização do usuário requer os seguintes componentes:

- Citrix Virtual Apps and Desktops 7 1909 ou posterior
- Virtual Delivery Agent (VDA), versão 1912 ou posterior
- Citrix Provisioning™, versão 1909 ou posterior
- Compartilhamento de Arquivos do Windows (SMB), ou Azure Files com autenticação AD local habilitada

Você pode implantar o recurso de Camada de personalização do usuário nas seguintes versões do Windows quando o SO é implantado como uma sessão única. O suporte é limitado a um único usuário em uma única sessão.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versão 1607 ou posterior
- Windows Server 2016 (Azure Files compatível)
- Windows Server 2019 (Azure Files compatível)
- Windows Server 2022 (Azure Files compatível)

Para Citrix Virtual Apps and Desktops 7, o uso de Azure Files com camadas de personalização do usuário é suportado no Windows Server 2022, Windows Server 2019, Windows Server 2016 e clientes Windows 10.

> **Nota:**
>
> Se você estiver usando um SO de servidor, apenas o VDI de Servidor é suportado. Para detalhes de implantação, consulte o artigo VDI de Servidor.

> A camada de personalização do usuário suporta apenas um usuário por vez por máquina, e então a máquina precisa ser reiniciada para redefinir os discos. Você não pode usar a camada de personalização do usuário com sistemas operacionais de servidor multi-sessão, apenas com sistemas de servidor de sessão única. A camada de personalização do usuário é compatível apenas com desktops não persistentes.

> Desinstale o recurso de camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

## Configurar seu compartilhamento de arquivos

O recurso de camada de personalização do usuário requer armazenamento Windows Server Message Block (SMB). Para criar um compartilhamento de arquivos do Windows, siga as etapas usuais para o sistema operacional Windows que você está usando.

Para saber mais sobre como usar o Azure Files com catálogos baseados em Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

## Recomendações

Siga as recomendações nesta seção para uma implantação bem-sucedida da camada de personalização do usuário.

### Microsoft System Center Configuration Manager (SCCM)

Se você estiver usando o SCCM com o recurso de camada de personalização do usuário, siga as diretrizes da Microsoft para preparar sua imagem em um ambiente VDI. Consulte este artigo do Microsoft TechNet para obter mais informações.

### Tamanho da camada de usuário

Uma camada de usuário é um disco com provisionamento dinâmico que se expande à medida que o espaço no disco é usado. O tamanho padrão permitido para uma camada de usuário é de 10 GB, o mínimo que recomendamos.

> **Nota:**
>
> Durante a instalação, se o valor for definido como zero (0), o tamanho padrão da camada de usuário será definido como 10 GB.

> Se você quiser alterar o tamanho da camada de usuário, pode inserir um valor diferente para a política **Tamanho da Camada de Usuário**. Consulte **Etapa 5: Criar políticas personalizadas de grupo de entrega**, em **Opcional: Clique em Selecionar ao lado de Tamanho da Camada de Usuário em GB.**

### Ferramentas para substituir o Tamanho da Camada de Usuário (Opcional)

Você pode substituir o Tamanho da Camada de Usuário usando uma ferramenta do Windows para definir uma cota no compartilhamento de arquivos da camada de usuário.

Use uma das seguintes ferramentas de cota da Microsoft para definir uma cota rígida no diretório da camada de usuário chamado **Users**:

- Gerenciador de Recursos do Servidor de Arquivos (FSRM)
- Gerenciador de Cotas

> **Nota:**
>
> Aumentar a cota afeta novas camadas de usuário e expande as existentes. Diminuir a cota afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

## Implantar uma camada de personalização do usuário

Ao implantar o recurso de personalização do usuário, você define as políticas no Web Studio. Em seguida, você atribui as políticas ao grupo de entrega vinculado ao catálogo de máquinas, onde o recurso é implantado.

Se você deixar a imagem mestra sem configuração de camada de personalização do usuário, os serviços permanecerão ociosos e não interferirão nas atividades de autoria.

Se você definir as políticas na imagem mestra, os serviços tentarão executar e montar uma camada de usuário dentro da imagem mestra. A imagem mestra exibirá comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, conclua as seguintes etapas nesta ordem:

- Etapa 1: Verifique a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Etapa 2: Prepare sua imagem mestre.
- Etapa 3: Crie um catálogo de máquinas.
- Etapa 4: Crie um grupo de entrega.
- Etapa 5: Crie políticas personalizadas de grupo de entrega.

> **Nota:**
>
> O primeiro login após a atualização do Windows 10 na imagem leva mais tempo do que o normal. A camada do usuário precisa ser atualizada para a nova versão do Windows 10, o que aumenta o tempo de logon.

### Etapa 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops esteja disponível para uso com este novo recurso. Para obter detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

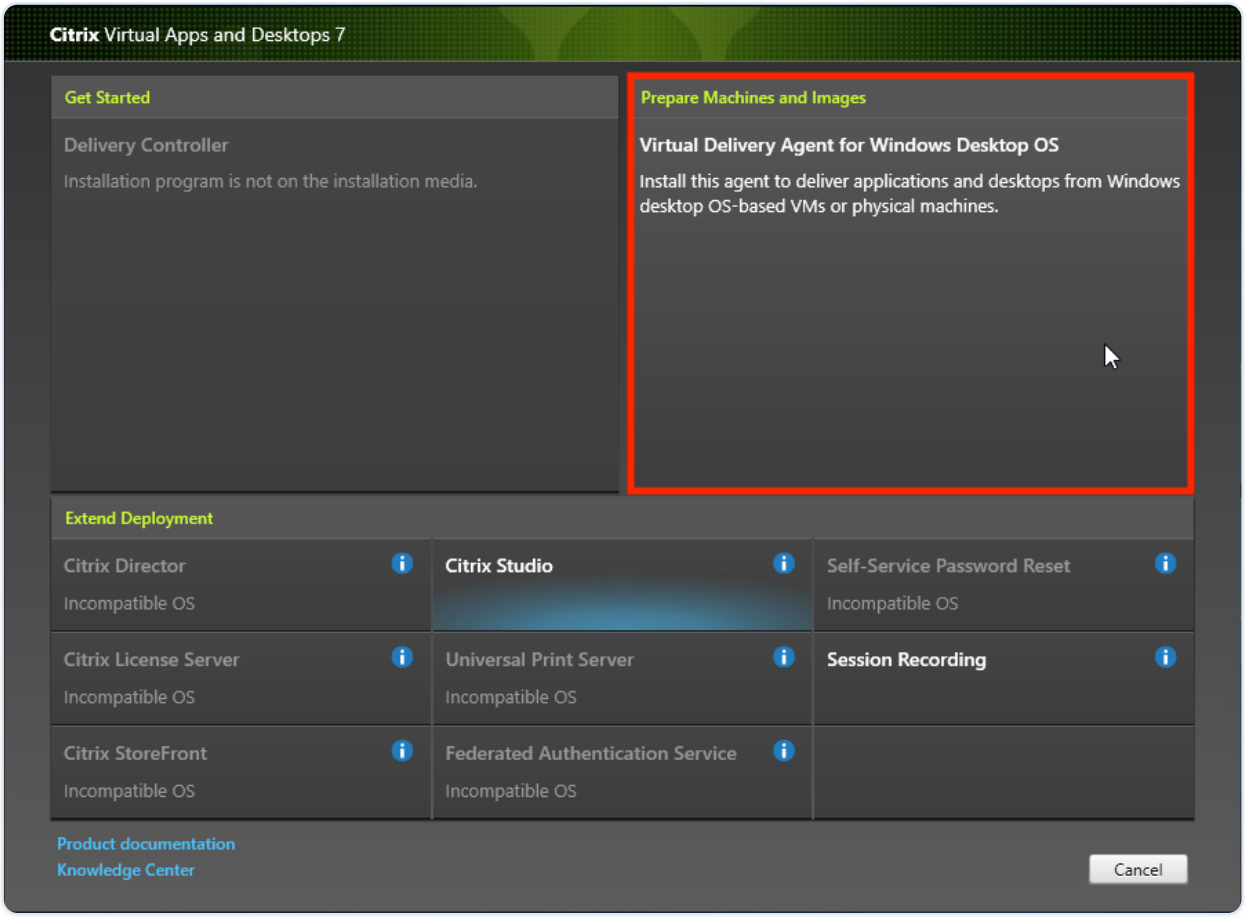
### Etapa 2: Prepare sua imagem mestra

Para preparar sua imagem mestre:

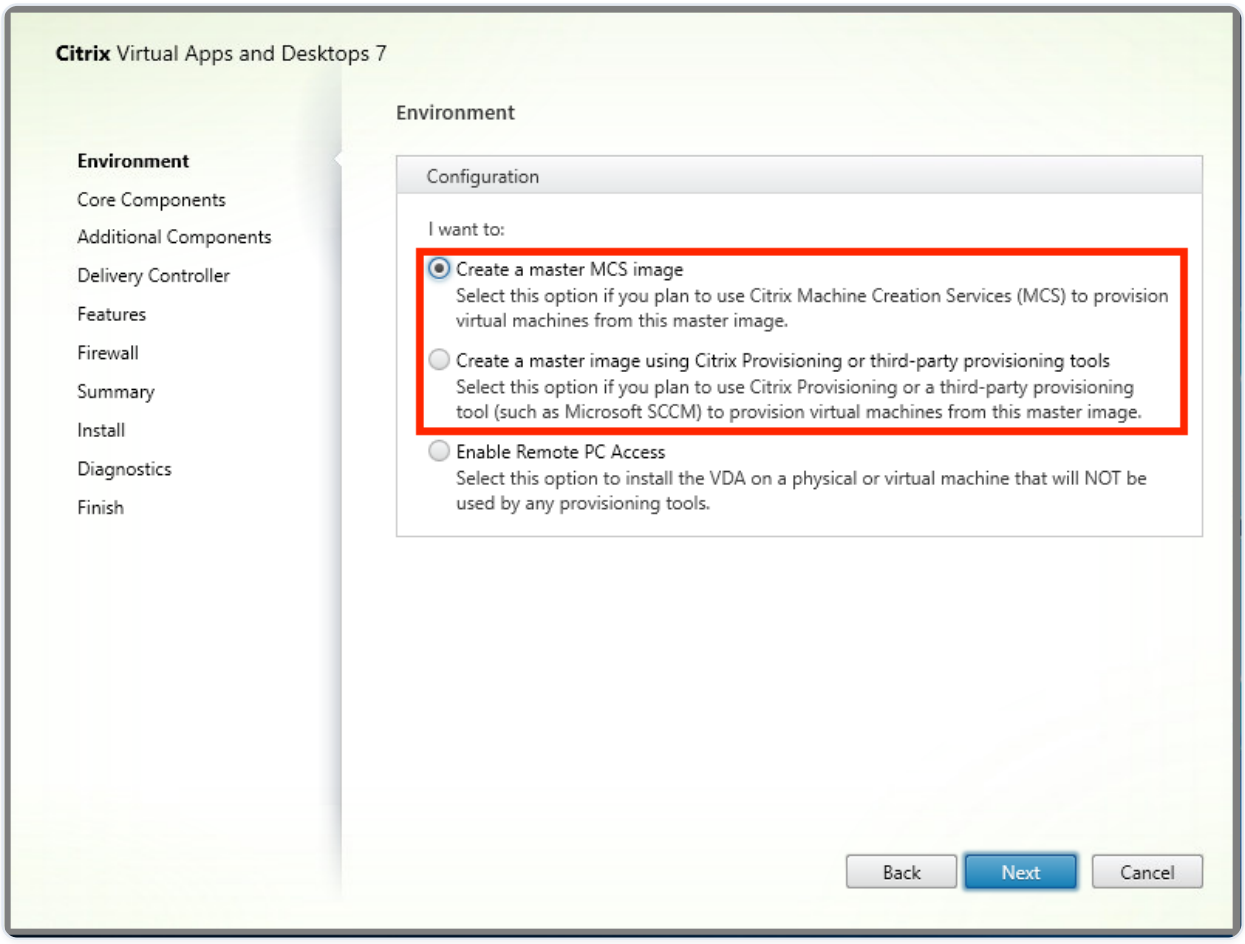
1. Localize a imagem mestre. Instale os aplicativos corporativos da sua organização e quaisquer outros aplicativos que seus usuários geralmente considerem úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Certifique-se de incluir o componente opcional, a **Camada de personalização do usuário**. Para obter detalhes, consulte as Opções de linha de comando para instalar um VDA.

3. Se você estiver usando o Windows 10, instale o Virtual Delivery Agent (VDA) 1912 ou posterior. Se uma versão mais antiga do VDA já estiver instalada, desinstale a versão antiga primeiro. Ao instalar a nova versão, certifique-se de selecionar e instalar o componente opcional, a **Camada de Personalização do Usuário Citrix**, da seguinte forma:

   a. Clique no bloco **Virtual Delivery Agent for Windows Desktop OS**:

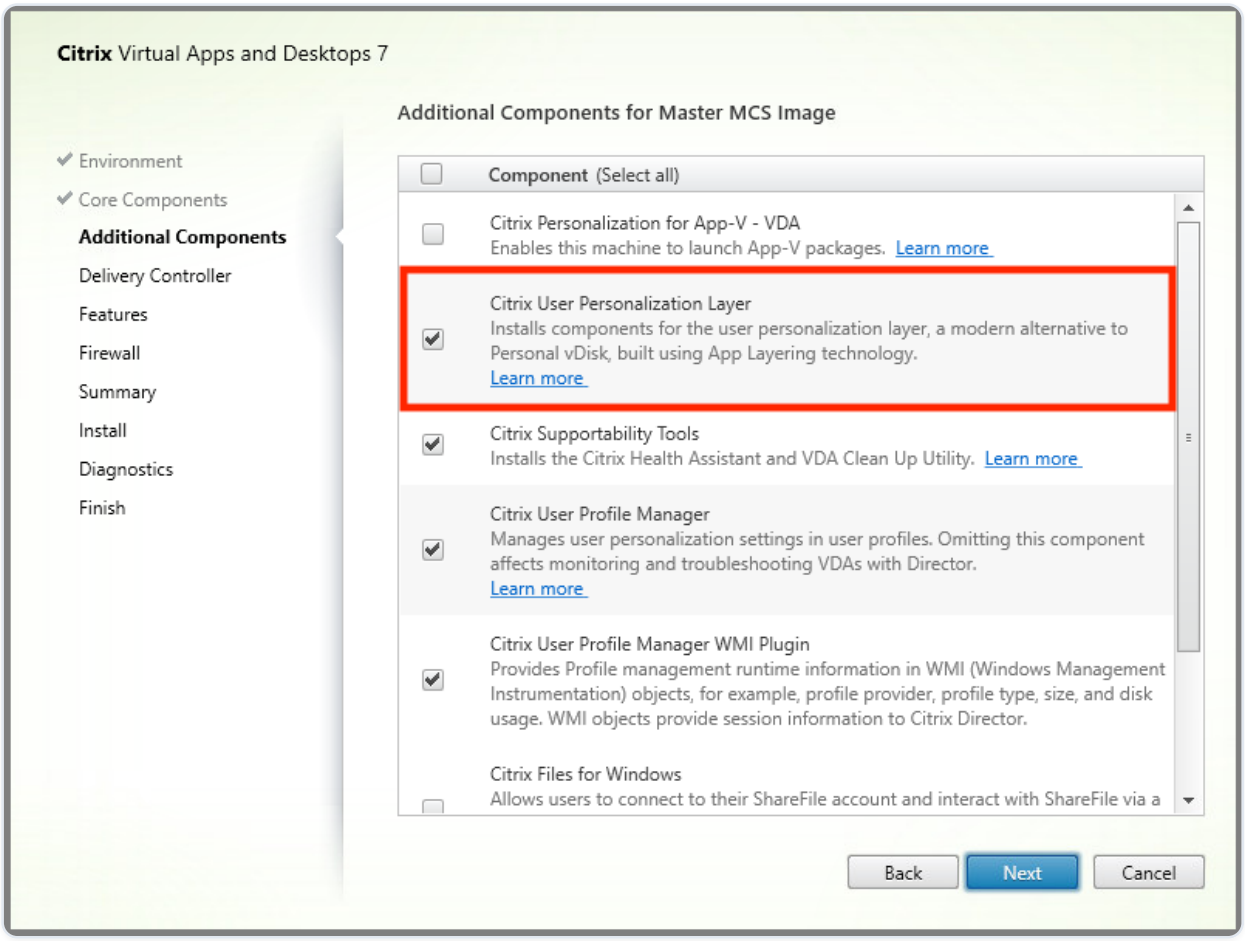



   a. **Ambiente:** Selecione **Criar uma imagem MCS mestre** ou **Criar uma imagem mestre usando o Citrix Provisioning ou ferramentas de provisionamento de terceiros**.




a. **Componentes Principais:** Clique em **Avançar**.

b. **Componentes Adicionais:** Marque **Camada de Personalização do Usuário Citrix**.




a. Clique nas telas de instalação restantes, configure o VDA conforme necessário e clique em **Instalar**. A imagem reinicia uma ou mais vezes durante a instalação.

4. Deixe as **atualizações do Windows** desativadas. O instalador da camada de personalização do usuário desativa as atualizações do Windows na imagem. Deixe as atualizações desativadas.

A imagem está pronta para ser carregada no Web Studio.

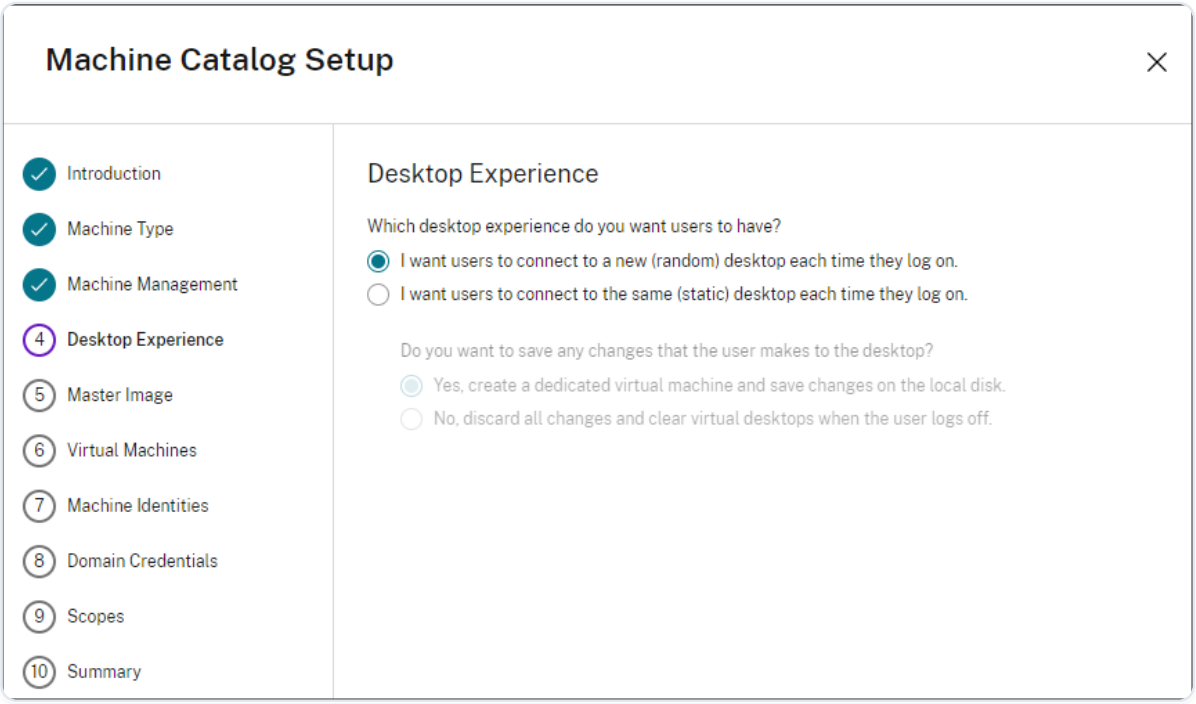
> **Nota:**
>
> Se você simplesmente deseja atualizar a camada de personalização do usuário (UPL), pode fazê-lo com uma versão mais recente da UPL e o pacote autônomo. Você não precisa atualizar o VDA.

### Etapa 3: Criar um catálogo de máquinas

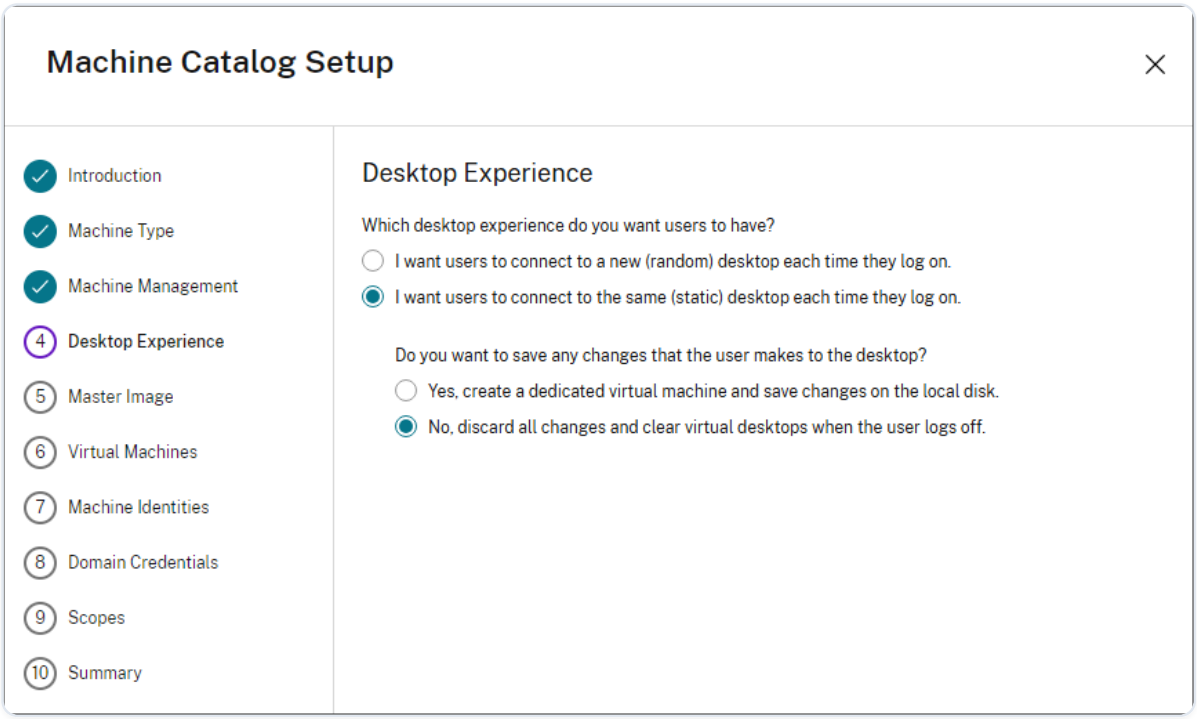
No Web Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

1. Selecione **Sistema Operacional** e defina-o como **SO de sessão única**.
2. Selecione **Gerenciamento de Máquinas** e defina-o como **Máquinas com gerenciamento de energia**. Por exemplo, máquinas virtuais ou PCs blade.
3. Selecione **Experiência de Área de Trabalho** e defina-o como tipo de catálogo **pooled-random** ou **pooled-static**, como nos exemplos a seguir:

   - **Pooled-random:**




   - **Pooled-static:** Se você selecionar pooled-static, configure as áreas de trabalho para descartar todas as alterações e limpar as áreas de trabalho virtuais quando o usuário fizer logoff, conforme mostrado na seguinte captura de tela:




**Nota:**

A camada de personalização do usuário não oferece suporte a catálogos pooled-static configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se você estiver usando o MCS, selecione **Imagem** e o instantâneo para a imagem criada na seção anterior.
5. Configure as propriedades restantes do catálogo conforme necessário para o seu ambiente.

### Etapa 4: Criar um grupo de entrega

Crie e configure um **grupo de entrega**, incluindo máquinas do catálogo de máquinas que você criou. Para obter detalhes, consulte Criar Grupos de Entrega.

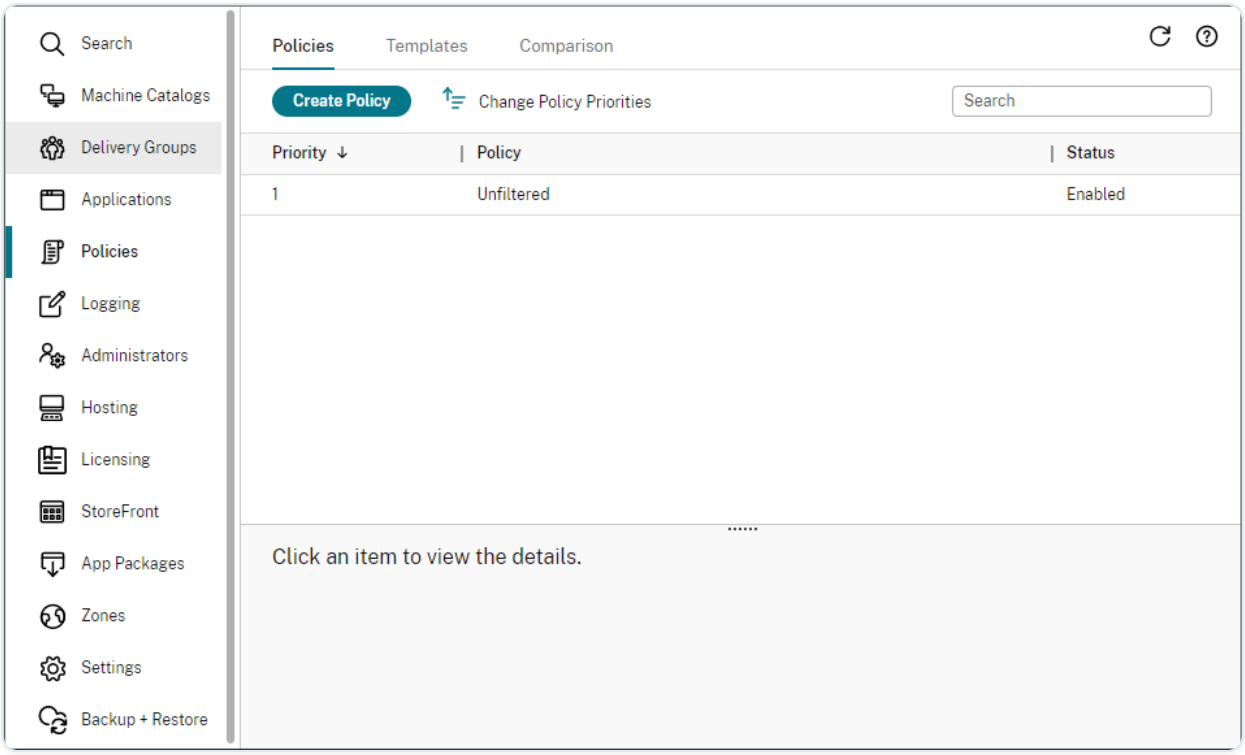
### Etapa 5: Criar políticas personalizadas de grupo de entrega

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, você usa os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- Qual o tamanho permitido para o crescimento dos discos da camada de usuário.

Para definir os parâmetros como políticas personalizadas do Citrix no Web Studio e atribuí-los ao seu grupo de entrega.

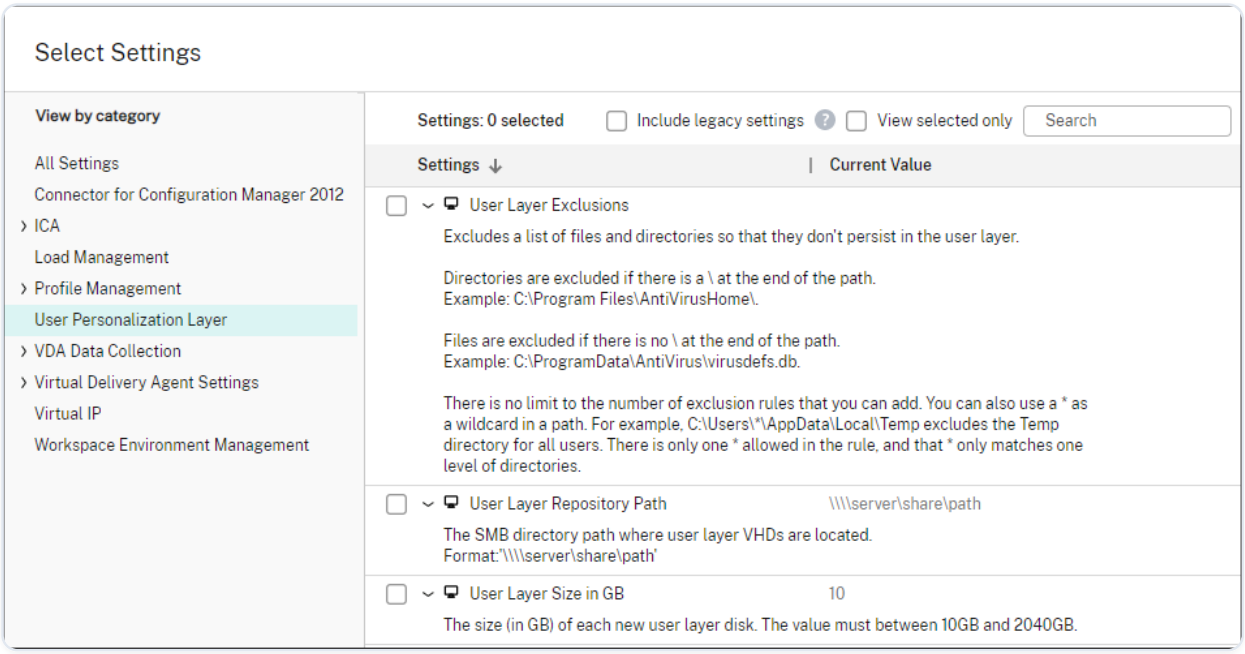
1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo:




2. Selecione **Criar Política** na barra de ações. A janela Criar Política é exibida.
3. Digite `user layer` no campo de pesquisa. As três políticas a seguir aparecem na lista de políticas disponíveis:

   - Exclusões de Camada de Usuário
   - Caminho do Repositório da Camada de Usuário
   - Tamanho da Camada de Usuário GB

   > **Nota:**
   >
   > Aumentar o tamanho afeta novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.



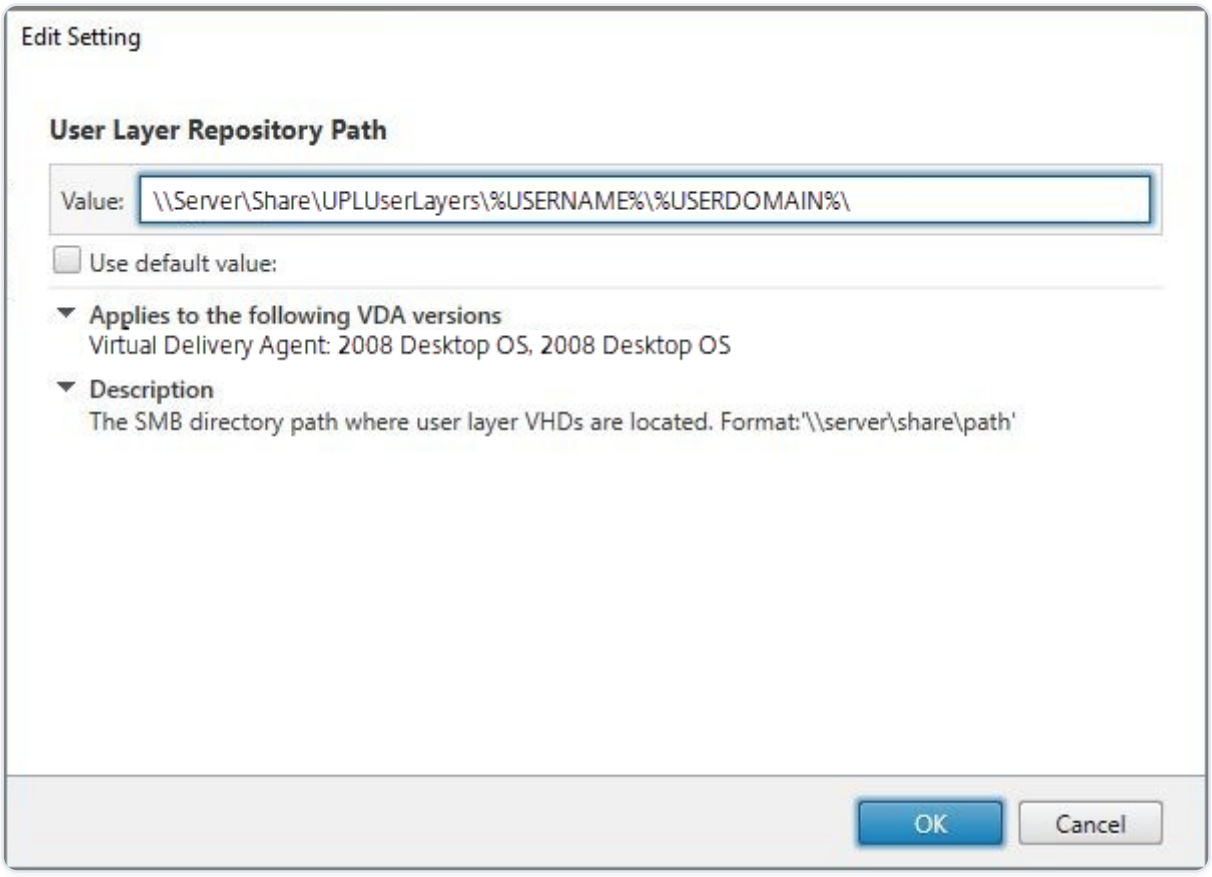

4. Marque a caixa de seleção ao lado de **Caminho do Repositório da Camada de Usuário** e clique em **Editar**. A janela **Editar Configuração** é exibida.
5. Insira um caminho no campo **Valor** e clique em **Salvar**:
   - **Formato do caminho:** `\\server-name-or-address\share-name\folder`
   - **Exemplo de caminho:** `\\Server\Share\UPLUsers`
   - **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho é: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



Você pode personalizar o caminho usando as variáveis `%USERNAME%` e `%USERDOMAIN%`, variáveis de ambiente da máquina e atributos do Active Directory (AD). Quando expandidas, essas variáveis resultam em caminhos explícitos.

Exemplo de variáveis de ambiente:

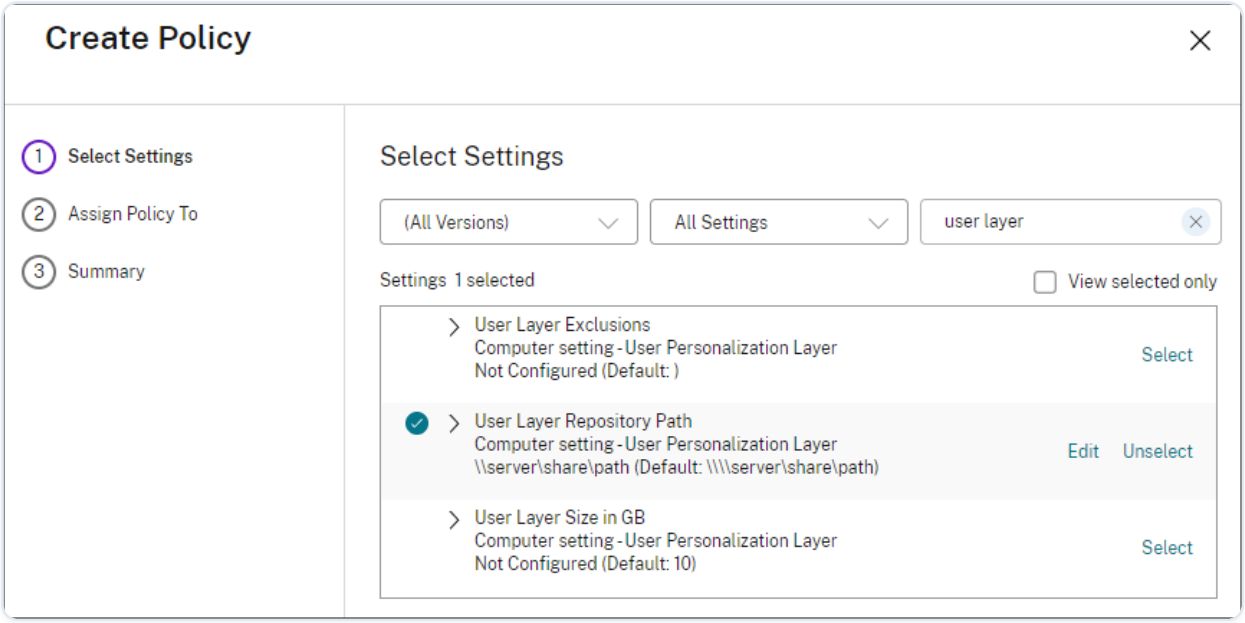
- **Formato do caminho:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Exemplo de caminho:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`




Exemplo de atributos AD personalizados:

- Formato do caminho: `\\Server-name-or-address\share-name\AD-attribute`
- Exemplo de caminho: `\\Server\share#sAMAccountName#`
- Exemplo de caminhos resultantes: `\\Server\share\JohnSmith` (se #sAMAccountName# for resolvido para JohnSmith para o usuário atual)

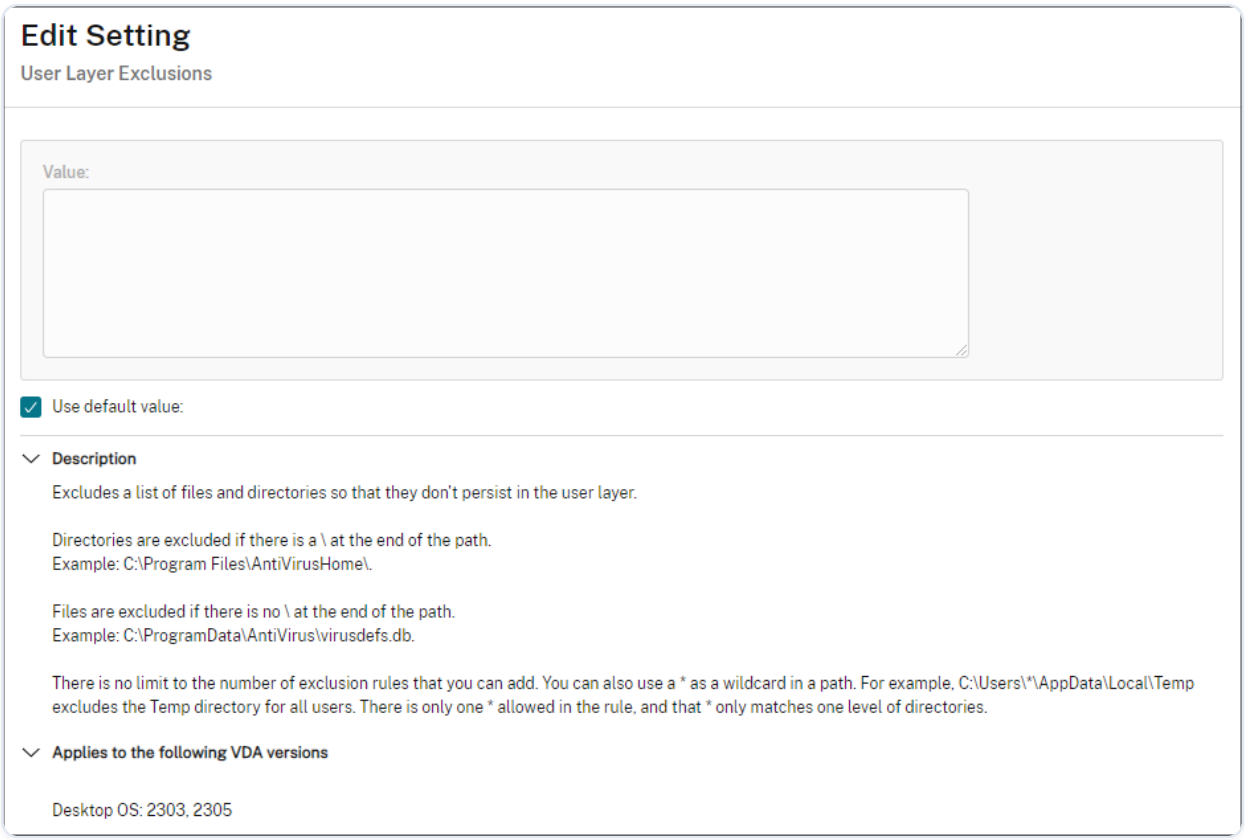
6. Opcional: Marque a caixa de seleção ao lado de **Tamanho da Camada de Usuário em GB** e clique em **Editar**:



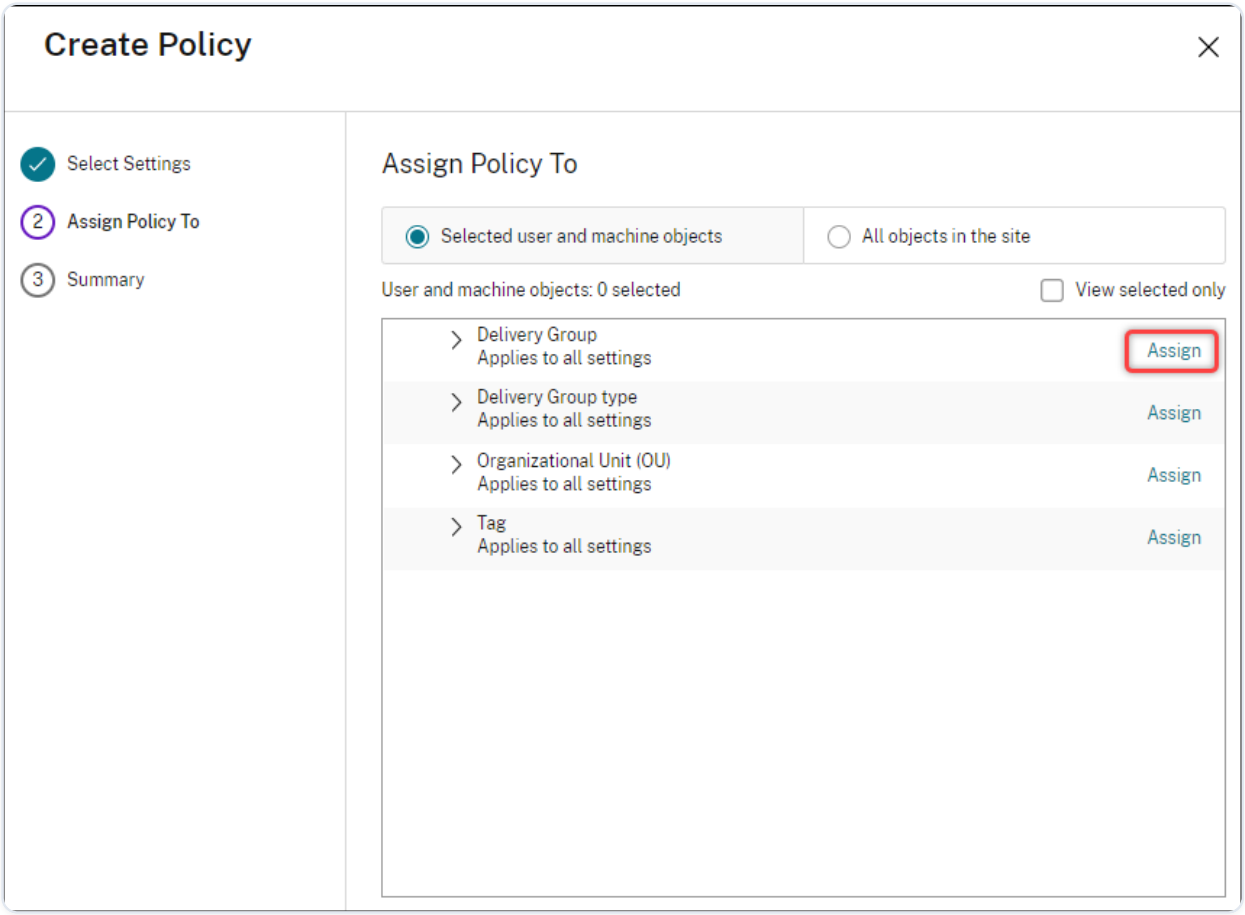

A janela Editar Configurações é exibida.

7. Opcional: Altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode atingir. Clique em **Salvar**.

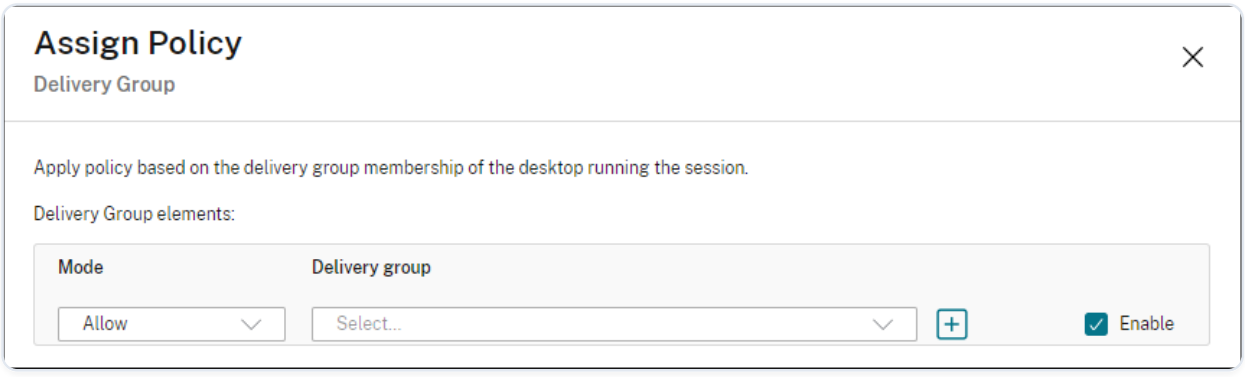
8. Opcional: Marque a caixa de seleção ao lado de **Exclusões da Camada de Usuário** e clique em **Editar**.



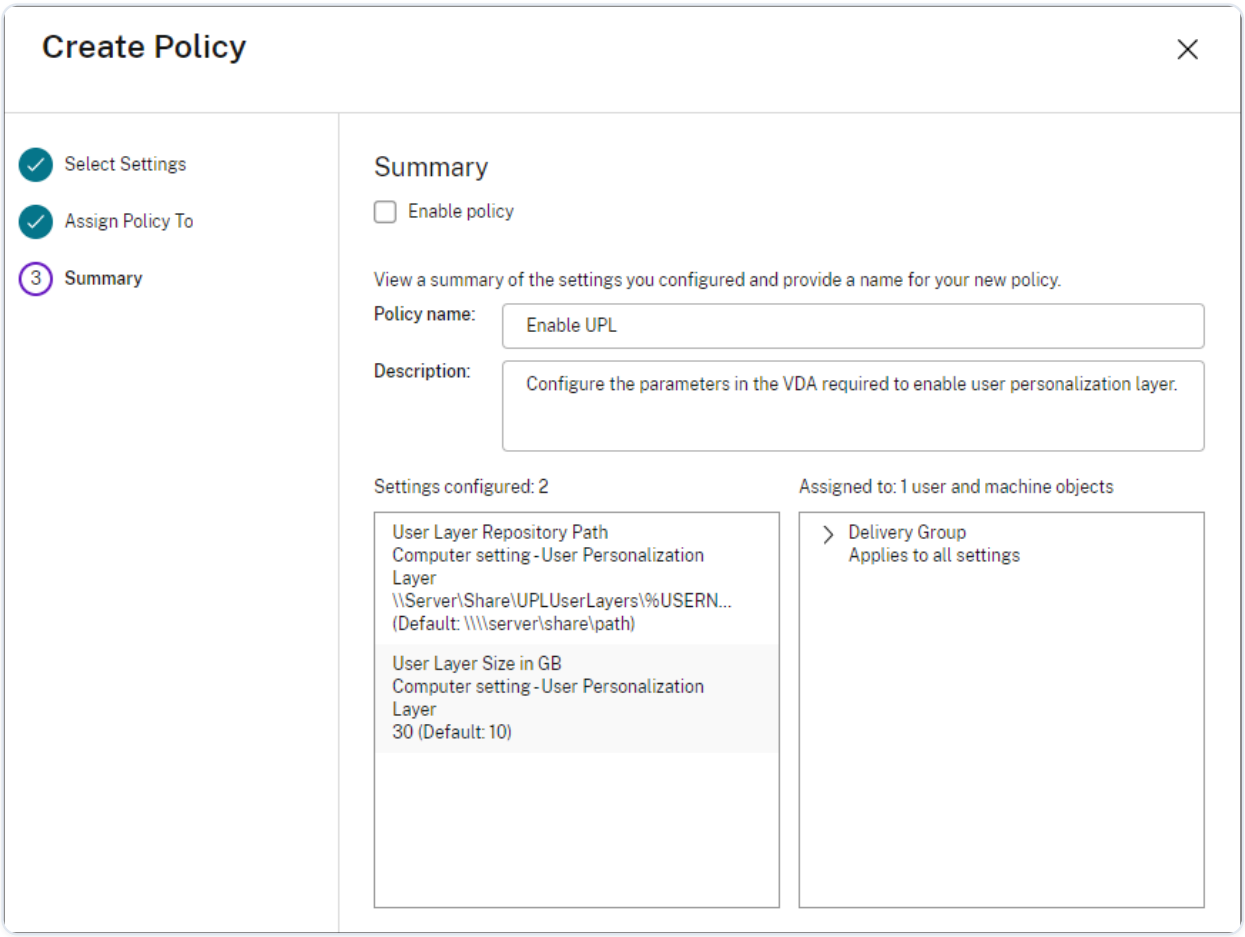
9. Opcional: Especifique os arquivos e pastas a serem excluídos e, em seguida, clique em **Salvar**. Para obter mais informações, consulte a documentação do Citrix App Layering.
10. Clique em **Avançar** para configurar os usuários e máquinas aos quais você deseja atribuir. Clique no link **Atribuir Grupo de Entrega** destacado nesta imagem:




11. No menu **Grupo de Entrega**, selecione o grupo de entrega criado na seção anterior. Clique em **OK**.




12. Insira um nome para a política. Marque a caixa de seleção para habilitar a política e clique em **Concluir**.




## Configurar configurações de segurança na pasta da camada de usuário

Como administrador de domínio, você pode especificar mais de um local de armazenamento para suas camadas de usuário. Crie uma subpasta `\Users` para cada local de armazenamento (incluindo o local padrão). Proteja cada local usando as seguintes configurações.

| NOME DA CONFIGURAÇÃO | VALOR | APLICAR A | |
|---|---|---|---|
| Criador/Proprietário | Modificar | Somente subpastas e arquivos | |
| Direitos do Proprietário | Modificar | Somente subpastas e arquivos | |
| Usuários ou grupo | Criar Pasta/Anexar Dados; Atravessar Pasta/Executar Arquivo; Listar Pasta/Ler Dados; Ler Atributos | Somente Pasta Selecionada | |

| NOME DA CONFIGURAÇÃO | VALOR | APLICAR A | |
|---|---|---|---|
| Sistema | Controle Total | Pasta Selecionada, Subpastas e Arquivos | |
| Administradores de Domínio e grupo de Administradores selecionado | Controle Total | Pasta Selecionada, Subpastas e Arquivos | |

## Mensagens da camada de usuário

Quando um usuário não consegue acessar sua camada de usuário, ele recebe uma destas mensagens de notificação.

- **Camada de Usuário em Uso**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Camada de Usuário Indisponível**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Sistema não redefinido após o logout do usuário**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

## Arquivos de log para usar na solução de problemas

O arquivo de log, ulayersvc.log, contém a saída do software da camada de personalização do usuário onde as alterações são registradas.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

## Reclamação de espaço da Camada de Usuário/UPL

Você pode usar a **reclamação de espaço da Camada de Usuário/UPL** para compactar automaticamente os arquivos VHDX toda vez que o usuário fizer logoff. Para obter mais informações, consulte Reclamação de espaço da Camada de Usuário/UPL

## Limitações

Tenha em mente as seguintes limitações ao instalar e usar o recurso de camada de personalização do usuário.

- NÃO *tente* implantar o software da camada de personalização do usuário em uma camada dentro do App Layering. Ou implante camadas de personalização do usuário no Citrix Virtual Apps and Desktops ou habilite camadas de usuário em um modelo de imagem do App Layering, não ambos. Qualquer um dos processos produz as camadas de usuário de que você precisa.
- Não *configure* o recurso de camada de personalização do usuário com catálogos de máquinas persistentes.
- Não *use* hosts de sessão.
- Não *atualize* o catálogo de máquinas com uma imagem executando uma nova instalação do SO (mesmo que seja a mesma versão do Windows 10). A melhor prática é aplicar as atualizações do SO na mesma imagem mestre usada ao criar o catálogo de máquinas.
- Não *use* drivers de tempo de inicialização ou qualquer outra personalização de inicialização precoce.
- Não *migre* dados PvD para o recurso de camada de personalização do usuário.
- Não *migre* camadas de usuário existentes do produto completo App Layering para o recurso de camada de personalização do usuário.
- Não *altere* o caminho SMB da camada de usuário para acessar camadas de usuário criadas usando uma imagem de SO mestre diferente.
- Quando um usuário faz logoff de uma sessão e depois faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Microsoft Software Center lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Indisponível** na segunda máquina.

  Para descobrir o status verdadeiro do aplicativo, instrua o usuário a selecionar o aplicativo no Software Center e clicar em **Instalar**. O SCCM então atualiza o status para o valor verdadeiro.

- O Software Center ocasionalmente para imediatamente após ser iniciado em um VDA que tem o recurso de camada de personalização do usuário habilitado. Para evitar esse problema, siga as recomendações da Microsoft para Implementando o SCCM em um ambiente VDI XenDesktop. Além disso, certifique-se de que o serviço `ccmexec` esteja em execução antes de iniciar o Software Center.
- Nas Políticas de Grupo (Configurações do Computador), as configurações da camada de usuário substituem as configurações aplicadas à imagem mestre. Portanto, as alterações feitas nas Configurações do Computador usando um GPO nem sempre estão presentes para o usuário no próximo login da sessão.

  Para contornar esse problema, crie um Script de Logon do Usuário que emita o comando:

  ```
  gpupdate /force
  ```

  Por exemplo, um cliente configurou o seguinte comando para ser executado em cada login de usuário:

  ```
  gpudate /Target:Computer /force
  ```

  Para obter melhores resultados, aplique as alterações nas Configurações do Computador diretamente na camada de usuário, depois que o usuário tiver feito login.
- Uma conta de usuário de domínio não deve ser o último usuário a ter feito login em uma imagem mestre. Caso contrário, as máquinas provisionadas a partir dessa imagem podem apresentar problemas.
- Certificados personalizados não persistem quando o UPL está ativado em um ambiente puro do Azure AD, devido a um problema subjacente no Windows em execução no Azure. Se a Microsoft corrigir esse problema em um aprimoramento futuro, atualizaremos este artigo.

# Remover componentes

Para remover componentes, a Citrix® recomenda usar o recurso do Windows para remover ou alterar programas. Alternativamente, você pode remover componentes usando a linha de comando ou um script na mídia de instalação.

Ao remover componentes, os pré-requisitos não são removidos e as configurações do firewall não são alteradas. Por exemplo, ao remover um Delivery Controller™, o software SQL Server e os bancos de dados não são removidos.

Se você atualizou um Controller de uma implantação anterior que incluía o Web Interface, você deve remover o componente Web Interface separadamente. Você não pode usar o instalador para remover o Web Interface.

Para obter informações sobre como remover recursos não mencionados abaixo, consulte a documentação do recurso.

## Preparação

Antes de remover um Controller, remova-o do site. Para obter detalhes, consulte Remover um Controller.

Feche o Studio e o Director antes de removê-los.

## Remover componentes usando o recurso do Windows para remover ou alterar programas

No recurso do Windows para remover ou alterar programas:

- Para remover um Controller, Studio, Director, License Server ou StoreFront, clique com o botão direito em **Citrix Virtual Apps *versão*** ou **Citrix Virtual Apps and Desktops™ *versão*** e selecione **Desinstalar**. O instalador será iniciado. Selecione os componentes a serem removidos.

  Alternativamente, você pode remover o StoreFront™ clicando com o botão direito em **Citrix StoreFront** e selecionando **Desinstalar**.
- Para remover um VDA, clique com o botão direito em **Citrix Virtual Delivery Agent *versão*** e selecione **Desinstalar**. O instalador será iniciado e você poderá selecionar os componentes a serem removidos. A máquina reinicia automaticamente após a remoção, por padrão.
- Para remover o Universal Print Server, clique com o botão direito em **Citrix Universal™ Print Server** e selecione **Desinstalar**.

## Remover componentes principais usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopServerSetup.exe`.

- Para remover um ou mais componentes, especifique as opções `/remove` e `/components`.
- Para remover todos os componentes, especifique a opção `/removeall`.

Para obter detalhes de comandos e parâmetros, consulte Instalar usando a linha de comando.

Por exemplo, o seguinte comando remove o Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

## Remover VDAs usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopVdaSetup.exe`.

- Para remover um ou mais componentes, use as opções `/remove` e `/components`. Por exemplo, para remover o VDA e o aplicativo Citrix Workspace, use `/remove /components vda,plugin`.
- A opção `/removeall` remove apenas o VDA. Ela não remove o aplicativo Citrix Workspace.

Para obter detalhes de comandos e parâmetros, consulte Instalar usando a linha de comando.

A máquina reinicia automaticamente após a remoção, por padrão.

Para remover VDAs usando um script no Active Directory, consulte Instalar ou remover VDAs usando scripts.

# Atualizar e migrar

## Introdução

**Observação:**

O sistema de licenciamento baseado em arquivo, tradicionalmente usado para ativar vários componentes locais, terá seu Fim de Vida (EOL) em April 15, 2026. O Serviço de Ativação de Licenças (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. O LAS será a única forma de ativar e licenciar componentes locais da Citrix após April 15, 2026. Para permanecer com suporte, sua implantação do Citrix Virtual Apps and Desktops deve estar em uma versão compatível com LAS. As versões mínimas de CVAD necessárias que são compatíveis com LAS são:

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

Se tiver dúvidas ou preocupações, entre em contato com o Suporte ao Cliente. A Citrix poderá limitar ou suspender sua Manutenção Citrix por não conformidade com esses requisitos, sem responsabilidade, além de quaisquer outros recursos que a Citrix possa ter por lei ou equidade. Esses requisitos não se aplicam onde proibido por lei ou regulamento.

**Observação:**

- **O Aviso de "Interseção de Versões"**

> Esteja ciente de que diferentes versões LTSR frequentemente se sobrepõem em seus ciclos de manutenção. Antes de iniciar uma atualização, você deve verificar a **Data de Lançamento** do seu Cumulative Update (CU) atual e do seu LTSR de destino (ou seu CU subsequente). Se a data de lançamento do seu ambiente atual for **posterior** à data de lançamento do LTSR de destino ou do CU do LTSR, a Citrix recomenda fortemente aguardar o próximo CU do LTSR mais recente. Proceder de outra forma pode fazer com que códigos mais antigos sobrescrevam atualizações de segurança existentes, patches de estabilidade e melhorias de recursos.
>
> - **A Cláusula de "Estado Não Suportado"**
>
>   Tentar atualizar para uma versão com uma data de lançamento anterior é tecnicamente considerado um **downgrade de componentes principais**. Esta configuração específica pode resultar em um status de **‘Sucesso Parcial’**.

> A atualização altera sua implantação para o Citrix Virtual Apps and Desktops 7 **Current Release (CR)** sem a necessidade de configurar novas máquinas ou sites. Isso é conhecido como uma atualização in-loco.

A atualização oferece acesso aos recursos e tecnologias mais recentes para os quais você é elegível. As atualizações também podem conter correções, esclarecimentos e aprimoramentos de versões anteriores.

## Visão geral da atualização

1. Revise o artigo Atualizar uma implantação antes de iniciar a atualização. Esta é a principal fonte de informação para aprender como se preparar e implementar uma atualização.
2. Certifique-se de que as datas atuais dos seus Serviços de Sucesso do Cliente são válidas e não expiraram. Para mais informações, consulte o artigo licenças de renovação dos Serviços de Sucesso do Cliente.
3. Conclua as orientações de preparação.
4. Execute os instaladores para atualizar os componentes principais.
5. Atualize os bancos de dados do sistema e o site.
6. Atualize os VDAs em imagens (ou diretamente nas máquinas).
7. Atualize outros componentes.

Cada etapa de preparação e atualização é detalhada em Atualizar uma implantação.

# Versões que você pode atualizar

Você pode atualizar para o Citrix Virtual Apps and Desktops 2402 LTSR a partir de:

- Virtual Apps and Desktops 2203 LTSR com ou sem CUs, até e incluindo CU5
- Virtual Apps and Desktops 1912 LTSR com ou sem CUs, até e incluindo CU9
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

> 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 seus requisitos específicos. Além disso, aconselhamos a revisão de toda a documentação relevante do produto, incluindo a lista de descontinuações e problemas conhecidos, para garantir uma transição suave. Essa abordagem ajuda a mitigar possíveis interrupções nos sistemas de produção e aprimora a experiência geral de atualização.
> - O Citrix Virtual Apps and Desktops 1912 LTSR em breve atingirá sua fase de fim de vida útil. Para 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 Virtual Apps and Desktops?**

  Para uma ilustração e descrição da sequência de atualização recomendada, consulte Sequência de atualização e Procedimento de atualização.

- **Meu site tem vários Delivery Controllers (em zonas diferentes). O que acontece se eu atualizar apenas alguns deles? Sou obrigado a atualizar todos os Controllers do 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?**

  Você quase sempre pode atualizar para a versão mais recente e pular as versões intermediárias, a menos que seja explicitamente declarado no artigo **Novidades** da versão para a qual você está atualizando.

- **Um cliente pode fazer upgrade de um ambiente Long Term Service Release (LTSR) para um Current Release?**

  Sim. Os clientes não são obrigados a permanecer em um Long Term Service Release por um período prolongado. Os clientes podem mover um ambiente LTSR para um Current Release, com base nos requisitos e recursos de negócios.

- **São permitidas versões mistas de componentes?**

  Em cada site, a Citrix recomenda atualizar todos os componentes para a mesma versão. Embora você possa usar versões anteriores de alguns componentes, nem todos os recursos da versão mais recente podem estar disponíveis. Para obter mais informações, consulte Considerações sobre ambientes mistos.

- **Com que frequência um Current Release deve ser atualizado?**

  Os Current Releases atingem o Fim da Manutenção (EOM) 6 meses após a data de lançamento. A Citrix recomenda que os clientes adotem o Current Release mais recente. Os Current Releases atingem o Fim da Vida Útil (EOL) 18 meses após a data de lançamento.

- **O que é recomendado: atualizar para LTSR ou CR?**

  As Current Releases (CRs) entregam os recursos e funcionalidades mais recentes e inovadores de virtualização de aplicativos, desktops e servidores. Isso permite que você permaneça na tecnologia de ponta e à frente da sua concorrência.

  As Long Term Service Releases (LTSRs) são ideais para grandes ambientes de produção corporativos que preferem manter a mesma versão base por um período estendido.

- **Preciso atualizar minhas licenças?**

  Certifique-se de que a data da licença atual não expirou e que é válida para a versão para a qual você está atualizando. Consulte CTX111618. Para obter informações sobre renovação, consulte licenças de renovação dos Customer Success Services.

- **Quanto tempo leva uma atualização?**

  O tempo necessário para atualizar uma implantação varia, dependendo da infraestrutura e da rede. Portanto, não podemos fornecer um tempo exato.

- **Quais são as melhores práticas?**

  Certifique-se de que você entende e segue as orientações de preparação.

- **Quais sistemas operacionais são suportados?**

  O artigo Requisitos do sistema para a versão para a qual você está atualizando lista os sistemas operacionais suportados.

  Se sua implantação atual usa sistemas operacionais que não são mais suportados, consulte Sistemas operacionais anteriores.

- **Quais versões do VMware vSphere (vCenter + ESXi) são suportadas?**

  CTX131239 lista os hosts e versões suportados, além de links para problemas conhecidos.

- **Quando minha versão chega ao fim da vida útil (EOL)?**

  Verifique a Matriz de Produtos.

- **Quais são os problemas conhecidos com a versão mais recente?**

  - Citrix Virtual Apps e Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - Citrix Workspace app para Windows

# Mais informações

As atualizações de implantação do **Long Term Service Release (LTSR)** usam Atualizações Cumulativas (CUs). Uma CU atualiza os componentes de linha de base do LTSR, e cada CU inclui seu próprio metainstaller.

Cada CU possui documentação dedicada. Por exemplo, para o LTSR 2203, verifique o link na página **Novidades** desse LTSR para a CU mais recente. Cada página de CU inclui informações de versão suportadas, instruções e um link para o pacote de download da CU.

# Migrar

## Migrar para a nuvem

Você pode usar a ferramenta de Configuração Automatizada para Citrix Virtual Apps and Desktops para migrar sua implantação local para a nuvem. Para obter mais informações, consulte Migrar para a Nuvem.

## Migração legada

A migração move dados de uma implantação anterior para uma versão mais recente. O processo inclui a instalação de componentes mais recentes e a criação de um novo site, a exportação de dados do farm antigo e, em seguida, a importação dos dados para o novo site.

Não há ferramentas ou scripts suportados para migrar versões do XenApp e XenDesktop, ou migrar versões anteriores do Citrix Virtual Apps and Desktops. A *atualização* é suportada para as versões do Citrix Virtual Apps and Desktops descritas nesta documentação do produto.

Para conteúdo de migração de versões anteriores do XenApp 6.x, consulte o seguinte. Os scripts não são suportados ou mantidos.

- Scripts de migração de código aberto para versões do XenApp 6.x estão disponíveis em `<https://github.com/citrix/xa65migrationtool>`. A Citrix não suporta nem mantém esses scripts de migração.
- Para **Changes in 7.x**, **Upgrade a XenApp 6.5 worker to a new VDA**, e **Migrate XenApp 6.x**, consulte o arquivo legado do Citrix Virtual Apps and Desktops em `<https://docs.citrix.com/pt-br/legacy-archive/citrix-virtual-apps-and-desktops.html>`.

# Atualizar uma implantação

> **Observação:**

> O sistema de licenciamento baseado em arquivo, tradicionalmente usado para ativar vários componentes locais, terá seu Fim de Vida (EOL) em April 15, 2026. O Serviço de Ativação de Licenças (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. O LAS será a única forma de ativar e licenciar componentes locais da Citrix após April 15, 2026. Para permanecer compatível, sua implantação do Citrix Virtual Apps and Desktops deve estar em uma versão compatível com LAS. As versões mínimas de CVAD necessárias que são compatíveis com LAS são:

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

Se você tiver dúvidas ou preocupações, entre em contato com o Suporte ao Cliente. A Citrix pode limitar ou suspender sua Manutenção Citrix por não conformidade com esses requisitos, sem responsabilidade, além de quaisquer outros recursos que a Citrix possa ter por lei ou equidade. Esses requisitos não se aplicam onde proibido por lei ou regulamento.

## Introdução

**Nota:**

Este artigo aborda atualizações para implantações que envolvem o Web Studio. Para obter informações sobre atualizações que envolvem o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops™ 7 2212 ou anterior.

Você pode atualizar certas implantações para versões mais recentes sem precisar configurar novas máquinas ou sites primeiro. Isso é chamado de atualização in-loco.

Para saber quais versões do Citrix Virtual Apps and Desktops você pode atualizar, consulte as Versões que você pode atualizar.

Antes de atualizar para qualquer uma das versões do Citrix Virtual Apps and Desktops, certifique-se de que suas datas atuais de Customer Success Services sejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo Licenças de renovação do Customer Success Services.

Para iniciar uma atualização, execute o instalador da nova versão para atualizar os componentes principais, VDAs e certos 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 VDA autônomos), se houver uma versão mais recente disponível. Para outros componentes que não são instalados com o instalador completo do produto (como Citrix Provisioning™ e Profile Management), consulte a documentação desse componente para obter orientação. Para atualizações de host, consulte a documentação apropriada.

Revise todas as informações neste artigo antes de iniciar uma atualização.

## Sequência de atualização

O diagrama a seguir mostra as etapas da sequência de atualização. Procedimento de atualização contém detalhes de cada etapa no diagrama.

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 uma das tarefas relacionadas ao provisionamento e ao grupo de entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

## Licenças de Direitos Híbridos

As licenças de Direitos Híbridos são licenças de assinatura baseadas em termo que são fornecidas, além da assinatura do serviço em nuvem, quando um cliente faz a transição ou upgrade de uma licença perpétua para uma assinatura de serviço em nuvem. Você também pode adquirir um complemento de Direitos Híbridos com suas assinaturas DaaS.

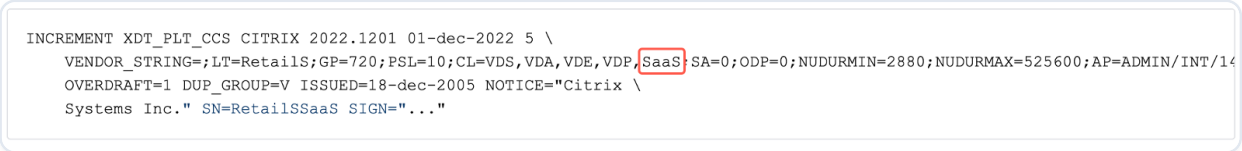
Se você tiver uma licença de Direitos Híbridos com um atributo SaaS, ao atualizar para o Citrix Virtual Apps and Desktops LTSR 2203 e posterior, você se tornará elegível para acessar recursos não disponíveis com o Citrix Virtual Apps and Desktops LTSR 1912. Esses recursos incluem provisionamento e hospedagem de cargas de trabalho em nuvens públicas, como Microsoft Azure, AWS EC2 e Google Cloud. Antes de implantar o novo arquivo de licença, atualize seu License Server para a versão mais recente; o não cumprimento deste pré-requisito pode causar erros ou recomendações durante as atualizações e criação do site.

Se você tiver acesso a uma licença de Direitos Híbridos sem atributo SaaS, siga estas etapas para obter acesso à nova licença de Direitos Híbridos com atributo SaaS:

**Nota:**

- Você receberá um e-mail com um novo código de licença. Para obter mais informações, consulte Usar código de acesso de licença.
- Suas licenças existentes são revogadas. As licenças revogadas devem ser excluídas dos License Servers, seguidas pela instalação de novas licenças. Para obter mais informações, consulte Excluir arquivos de licença.

1. Acesse o portal citrix.com Gerenciar Licenças e baixe o novo arquivo de licença de Direitos Híbridos com direitos de provisionamento em nuvem ativados (atributo SaaS). Para obter mais informações, consulte Baixar licenças. A imagem a seguir mostra o arquivo de licença de Direitos Híbridos com atributo SaaS na seção Increments.




2. Instale o arquivo de licença de Direitos Híbridos no License Server. Para obter mais informações, consulte Instalar licenças.
3. Se houver uma alteração nas edições ou no modelo da licença, certifique-se de executar o comando do broker para definir a edição e o modelo e, em seguida, iniciar a atualização in-loco. Para obter mais informações sobre os comandos do Broker, consulte a seção Broker PowerShell SDK.

Para obter mais informações sobre o suporte a nuvem pública com o Citrix Virtual Apps and Desktops Current Releases e Long Term Service Releases, consulte CTX270373.

## Procedimento de atualização

A maioria dos componentes principais 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 do instalador completo do produto, faça logon na máquina e, em seguida, insira a mídia ou monte a unidade ISO para a nova versão. Clique duas vezes em **AutoSelect**.
- Para usar a interface de linha de comando, emita o comando apropriado. Consulte Instalar usando a linha de comando.

### Etapa 1: Preparar

Antes de iniciar uma atualização, certifique-se de que está pronto. Leia e conclua todas as tarefas necessárias:

- Remover PVD, AppDisks™ e hosts não suportados
- VDAs que possuem componentes PvD ou AppDisk
- Limitações
- Considerações sobre ambiente misto
- Sistemas operacionais anteriores
- Preparação
- Testes preliminares do site
- Verificação da versão do SQL Server

### Etapa 2: Atualizar o License Server

Se a instalação tiver uma nova versão do software Citrix License Server, atualize este componente primeiro antes de qualquer outro componente.

Se você ainda não determinou se seu License Server é compatível com a nova versão, é essencial que você execute o instalador no License Server antes de atualizar quaisquer outros componentes principais.

### Etapa 3: Atualizar o StoreFront™

Se a mídia de instalação contiver uma nova versão do software StoreFront, execute o instalador na máquina que contém o servidor StoreFront.

- Na interface gráfica, escolha **Citrix StoreFront** na seção **Estender implantação**.
- Na linha de comando, execute `CitrixStoreFront-x64.exe`, que está disponível na pasta `x64` da mídia de instalação do Citrix Virtual Apps and Desktops.

### Etapa 4: Atualizar o Director

Se a mídia de instalação contiver uma nova versão do software Director, execute o instalador na máquina que contém o Director.

### Etapa 5: Atualizar o Citrix Provisioning

A mídia de instalação do Citrix Provisioning está disponível separadamente da mídia de instalação do Citrix Virtual Apps and Desktops. Para saber como instalar e atualizar o servidor Citrix Provisioning e o software do dispositivo de destino, consulte a documentação do produto Citrix Provisioning.

### Etapa 6: Atualizar metade dos Delivery Controllers

Por exemplo, se o seu site tiver quatro Controllers, execute o instalador em dois deles.

Deixar metade dos Controllers ativos permite que os usuários acessem o site. Os VDAs podem se registrar nos Controllers restantes. Pode haver momentos em que o site tenha capacidade reduzida porque menos Controllers estão disponíveis. A atualização causa apenas uma breve interrupção no estabelecimento de novas conexões de cliente durante as etapas finais de atualização do banco de dados. Os Controllers atualizados não podem processar solicitações até que todo o site seja atualizado.

Se o seu site tiver apenas um Controller, ele ficará inoperante durante a atualização.

Testes preliminares do site são executados no primeiro Controller, antes do início da atualização real. Para obter detalhes, consulte Testes preliminares do site.

### Passo 7: Atualizar o Studio

Se você ainda não atualizou o Web Studio (porque 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, vá para o servidor do Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegar para Página Inicial > Sites > Site Padrão, e selecione **Reiniciar** no painel Gerenciar Site.

### Passo 8: Reiniciar o Studio

Reinicie o Web Studio atualizado. O processo de atualização é retomado automaticamente.

### Passo 9: Atualizar banco de dados e site

> **Nota:**
>
> Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer uma das tarefas relacionadas ao provisionamento e grupo de entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

> Verifique Preparação para as permissões necessárias para atualizar o esquema dos bancos de dados do SQL Server.

- Se você tiver permissão suficiente para atualizar o esquema do banco de dados do SQL Server, poderá iniciar uma atualização automática do banco de dados. Continue com Atualizar o banco de dados e o site automaticamente.
- Se você não tiver permissões de banco de dados suficientes, poderá iniciar uma atualização manual que usa scripts e prosseguir com a ajuda do seu administrador de banco de dados (alguém que tenha as permissões necessárias). Para uma atualização manual, o usuário do Studio gera os scripts e, em seguida, executa os scripts que habilitam e desabilitam os serviços. O administrador do banco de dados executa outros scripts que atualizam o esquema do banco de dados, usando o utilitário SQLCMD ou o SQL Server Management Studio no modo SQLCMD. Continue com Atualizar o banco de dados e o site manualmente.
- Se você tiver uma implantação multi-zona 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 pode falhar.

A Citrix recomenda fortemente que você faça backup do banco de dados antes de atualizar. Consulte CTX135207. Durante uma atualização do banco de dados, os serviços do produto são desabilitados. Durante esse período, os Controllers não podem intermediar novas conexões para o site, portanto, planeje cuidadosamente.

#### Atualizar o banco de dados e o site automaticamente

1. Inicie o Studio recém-atualizado.

2. Indique que deseja iniciar a atualização do site automaticamente e confirme que está pronto.

A atualização do banco de dados e do site prossegue.

#### Atualizar o banco de dados e o site manualmente

1. Inicie o Studio recém-atualizado.
2. Indique que deseja atualizar o site manualmente. O assistente verifica a compatibilidade do License Server e solicita confirmação.
3. Confirme que você fez backup do banco de dados.

   O assistente gera e exibe os scripts e uma lista de verificação das etapas de atualização. Se o esquema de um banco de dados não tiver sido alterado desde a versão do produto que está sendo atualizada, esse script não será gerado. Por exemplo, se o esquema do banco de dados de log não for alterado, o script `UpgradeLoggingDatabase.sql` não será gerado.
4. Execute os seguintes scripts na ordem mostrada.

   - `DisableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para desabilitar os serviços do produto.
   - `UpgradeSiteDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Site
   - `UpgradeMonitorDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Monitor.
   - `UpgradeLoggingDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados de Log de Configuração. Execute este script somente se este banco de dados for alterado (por exemplo, após aplicar um hotfix).
   - `EnableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para habilitar os serviços do produto.

   Após a conclusão da atualização do banco de dados e a habilitação dos serviços do produto, o Studio testa automaticamente o ambiente e a configuração e, em seguida, gera um relatório HTML. Se problemas forem identificados, você poderá restaurar o backup do banco de dados. Após resolver os problemas, você pode atualizar o banco de dados novamente.
5. Após concluir as tarefas da lista de verificação, clique em **Concluir atualização**.

### Etapa 10: Atualizar os Delivery Controllers restantes

No Studio recém-atualizado, selecione **Citrix Studio** *nome-do-site* no painel de navegação. Na guia **Tarefas Comuns**, selecione **Atualizar Delivery Controllers restantes**.

**Nota:**

Para que **Atualizar Delivery Controllers restantes** esteja disponível, crie pelo menos um catálogo de máquinas e um grupo de entrega para o site.

Após concluir a atualização e confirmar a conclusão, feche e reabra o Studio. O Studio pode solicitar uma atualização extra do site para registrar os serviços do Controller no site ou para criar um ID de zona, se ele não existir.

### Etapa 11: Atualizar VDAs

**Importante:**

Se você estiver atualizando um VDA para a versão 1912 ou posterior, consulte Atualizando VDAs para 1912 ou posterior.

Execute o instalador do produto nas máquinas que contêm VDAs.

Se você usou o Machine Creation Services™ e uma imagem mestre para criar máquinas, vá para o seu host e atualize o VDA na imagem mestre. Você pode usar qualquer um dos instaladores de VDA disponíveis.

- Para orientação sobre a interface gráfica, consulte Instalar VDAs.
- Para orientação sobre a linha de comando, consulte Instalar usando a linha de comando.

Se você usou o Citrix Provisioning para criar máquinas, consulte a documentação do produto Citrix Provisioning para obter orientação sobre a atualização.

### Etapa 12: Atualizar catálogos de máquinas e Delivery Groups

- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar Delivery Groups que usam máquinas com VDAs atualizados.

### Etapa 13: Após a atualização

Atualize outros componentes em sua implantação. Para obter orientação, consulte a seguinte documentação do produto:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

Se você precisar substituir o software Microsoft SQL Server Express LocalDB por uma versão posterior, consulte Substituir SQL Server Express LocalDB.

## Atualização do esquema de banco de dados

Ao atualizar sua implantação, vários esquemas de banco de dados podem ser atualizados. A tabela a seguir lista quais esquemas de banco de dados são atualizados no processo:

| From\To | 1912 CU1 | 1912 CU2 | 1912 CU3 | 1912 CU4 | 1912 CU5 | 2203 |
|---|---|---|---|---|---|---|
| 7.15 RTM or 7.15 CU releases | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 RTM | Config | Site, Config | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU1 | | Site | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU2 | | | Site, Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU3 | | | | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging |
| 1912 CU4 | | | | | Site, Config | Site; Monitor; Config; Logging |
| 1912 CU5 | | | | | | Site; Monitor; Config; Logging |
| 2112 | | | | | | Site; Monitor; Config |

Definição dos termos:

- Site: Datastore do Site. A atualização do esquema de banco de dados é feita no Datastore do Site.
- Monitor: Datastore do Monitor. A atualização do esquema de banco de dados é feita no Datastore do Monitor.
- Config: Tabela de configuração. A versão do Desktop Studio, as informações de licenciamento ou ambos são atualizados na tabela de configuração.
- Registro: Datastore de registro. A atualização do dbschema é feita no Datastore de registro.

# Atualizar VDAs para 2203 ou posterior

Se o componente Personal vDisk (PvD) foi instalado em um VDA, esse VDA não pode ser atualizado para a versão 2203 ou posterior. Para usar o novo VDA, você deve desinstalar o VDA atual e, em seguida, instalar o novo VDA.

Esta instrução se aplica mesmo que você nunca tenha usado o PvD.

Veja como o componente PvD pode ter sido instalado em versões anteriores:

- Na interface gráfica do instalador do VDA, o PvD era uma opção na página **Componentes Adicionais**.
- Na linha de comando, a opção `/baseimage` instalou o PvD. Se você especificou esta opção, ou usou um script que continha esta opção, o PvD foi instalado.

Se você não sabe se o seu VDA tem o PvD instalado, execute o instalador para o novo VDA (2203 ou posterior) na máquina ou imagem.

- Se o PvD estiver instalado, uma mensagem aparecerá, indicando que há um componente incompatível.
  - Na interface gráfica, clique em **Cancelar** na página que contém a mensagem e, em seguida, confirme que deseja fechar o instalador.
  - Na CLI, o comando simplesmente falha com a mensagem exibida.
- Se o PvD não estiver instalado, a atualização prossegue.

### O que fazer

Se o VDA não tiver o PvD instalado, siga o procedimento de atualização usual.

Se o VDA tiver PvD instalado:

1. Desinstale o VDA atual.
2. Instale o novo VDA.

Se você quiser continuar usando o PvD em suas máquinas Windows 10 (1607 e anteriores, sem atualizações), o VDA 7.15 LTSR é a versão mais recente suportada.

> **Nota:**

> *Posso usar o Personal vDisk com desktops Windows 7 no XenApp e XenDesktop 7.15 LTSR?*

> A Citrix excluiu o Personal vDisk (PvD) do XenApp e XenDesktop 7.6 LTSR, o que foi anunciado em janeiro de 2016. Além disso, a Citrix anunciou a descontinuação da tecnologia PvD e recomenda que os clientes comecem a usar o Citrix App Layering daqui para frente. O Citrix App Layering (versão 4.4 e posterior) é um componente compatível do XenApp e XenDesktop 7.15 LTSR. No entanto, para ajudar os clientes com implantações PvD existentes no Windows 7 a migrar para a tecnologia Citrix App Layering, a Citrix decidiu fornecer suporte por tempo limitado para implantações PvD para desktops Windows 7 por meio das Atualizações Cumulativas (CUs) do XenApp e XenDesktop 7.15 LTSR até Jan 14, 2020. O componente PvD será removido das CUs LTSR e não será suportado após Jan 14, 2020. Além disso, o uso de PvD para Windows 7 após Jan 14, 2020 tornará os sites LTSR não conformes. Além disso, o PvD para Windows 10 continua a ser excluído do 7.15 LTSR. Portanto, os clientes não devem usá-lo com seus sites 7.15 LTSR.

## Remover PvD, AppDisks e hosts não suportados

As seguintes tecnologias e tipos de host não são suportados em implantações do Citrix Virtual Apps and Desktops 7 Current Release:

- **Personal vDisks (PvD)** para armazenar dados ao lado das VMs dos usuários em catálogos. O recurso de camada de personalização do usuário agora lida com a persistência do usuário.
- **AppDisks** para gerenciar aplicativos usados em Delivery Groups.
- **Tipos de host:** Azure Classic, CloudPlatform (o produto Citrix original).
    - Para tipos de host suportados nesta versão, consulte Requisitos do sistema.
    - Para obter informações sobre maneiras alternativas de continuar usando ARM e AWS, consulte CTX270373.

Se sua implantação atual usa PvDs ou AppDisks, ou tem conexões com tipos de host não suportados (por exemplo, Microsoft Azure Classic), você pode atualizar para a versão 2006 (ou versões suportadas posteriores) somente após remover os itens que usam essas tecnologias. Se sua implantação atual usa conexões de host de nuvem pública (por exemplo, AWS), certifique-se de ter a Licença de Direitos Híbridos antes de atualizar. Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a

atualização pausa ou para, e uma mensagem explicativa aparece. Os logs do instalador contêm detalhes.

Para ajudar a garantir uma atualização bem-sucedida, revise e siga as orientações aplicáveis para remover os itens não suportados.

- Remover PvD(#remove-pvd)
- Remover AppDisks(#remove-appdisks)
- Remover itens de host não suportados(#remove-unsupported-host-items)

Mesmo que você não tenha usado PvD ou AppDisks em sua implantação, MSIs relacionados podem ter sido incluídos em uma instalação ou atualização anterior do VDA. Antes de atualizar seus VDAs para a versão 2006 (ou uma versão posterior compatível), 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 possuem componentes PvD ou AppDisks.

### Remover PvD

Uma atualização de implantação não pode ser bem-sucedida até que você remova todas as máquinas configuradas para usar PvD. Isso afeta catálogos e Delivery Groups.

Para remover PvD de grupos e catálogos:

1. No Studio, se um Delivery Group contiver máquinas de um catálogo que usa PvD, remova essas máquinas do grupo.
2. No Studio, exclua todos os catálogos que contêm máquinas que usam PvD.

**Atualizações de VDA:** A atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores do VDA detectam. Para obter detalhes, consulte VDAs que possuem componentes PvD ou AppDisks.

### Remover AppDisks

Uma atualização de implantação não pode prosseguir até que você remova os AppDisks de todos os Delivery Groups que os utilizam, e então 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 Ações.
3. Clique na ação que remove o AppDisk do grupo.
4. Repita os passos 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 os passos 5 e 6 para cada AppDisk.

**Atualizações de VDA:** A atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA detectam. Para obter detalhes, consulte VDAs que possuem componentes PvD ou AppDisks.

### Remover itens de host não suportados

Uma atualização de implantação para a versão 2006 (ou versão suportada posterior) não pode prosseguir se o site tiver conexões com tipos de host não suportados, como Citrix CloudPlatform ou Microsoft Azure Classic. Conclua as seguintes tarefas antes de tentar uma atualização.

No Studio:

- Exclua todas as conexões para hosts não suportados.
- Se um Grupo de Entrega contiver máquinas de um catálogo criado com uma imagem mestre de um host não suportado, remova essas máquinas do grupo.
- Exclua todos os catálogos que foram criados usando uma imagem mestre de um host não suportado.

### VDAs que possuem componentes PvD ou AppDisks

Se os componentes que habilitam as tecnologias PvD e AppDisks estiverem instalados em um VDA, esse VDA não poderá ser atualizado até que esses componentes sejam removidos.

> **Nota:**
>
> Ao atualizar para a versão 1912, você precisava desinstalar o VDA atual e, em seguida, instalar o novo VDA. Nesta versão, é perguntado se você deseja que a Citrix remova o componente e, em seguida, continue a atualização.

> Os componentes AppDisk e PvD podem ter sido instalados em versões anteriores do VDA, mesmo que você nunca tenha usado essas tecnologias:

- Interface gráfica: Nos instaladores do VDA, a página **Componentes Adicionais** continha a opção **Citrix AppDisk / Personal vDisk**. As versões 7.15 LTSR e 7.x anteriores habilitavam

essa opção por padrão. Assim, se você aceitou os padrões (ou habilitou explicitamente a opção em qualquer versão que a oferecesse), esse componente foi instalado.

- CLI: A especificação da opção `/baseimage` instalou o componente.

**O que fazer**

Se o instalador do VDA não detectar os componentes AppDisks ou PvD no VDA atualmente instalado, a atualização prossegue normalmente.

Se o instalador detectar componentes AppDisks ou PvD no VDA atualmente instalado:

- Interface gráfica: A atualização é pausada. Uma mensagem pergunta se você deseja que os componentes não suportados sejam removidos automaticamente. Se você clicar em **OK**, os componentes são removidos automaticamente e a atualização prossegue.
- CLI: Para evitar falha de comando, inclua as seguintes opções no comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

## Limitações

As seguintes limitações se aplicam às atualizações:

- **Instalação seletiva de componentes:** Se você instalar ou atualizar quaisquer componentes para a nova versão, mas optar por não atualizar outros componentes (em máquinas diferentes) que exigem atualização, o Studio o lembrará. Por exemplo, digamos que uma atualização inclua novas versões do Controller e do Studio. Você atualiza o Controller, mas não executa o instalador na máquina onde o Studio está instalado. O Studio não permitirá que você continue a gerenciar o site até que você atualize o Studio.

  Você não precisa atualizar os VDAs, mas a Citrix recomenda atualizar todos os VDAs para permitir que você use todos os recursos disponíveis.
- **Versões de Lançamento Antecipado ou Pré-visualização Tecnológica:** Não é possível atualizar a partir de uma versão de Lançamento Antecipado, Pré-visualização Tecnológica ou pré-visualização.
- **Componentes em sistemas operacionais anteriores:** Não é possível instalar VDAs atuais em sistemas operacionais que não são mais suportados pela Microsoft ou Citrix. Para obter mais informações, consulte Sistemas operacionais anteriores.
- **Ambientes/sites mistos:** Se você precisar continuar a executar sites de versões anteriores e sites de versões atuais, consulte Considerações sobre ambientes mistos.

- **Seleção de produto:** Ao atualizar de uma versão anterior, você não escolhe ou especifica o produto (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) que foi definido durante a instalação.

## Considerações sobre ambientes mistos

Ao fazer o upgrade, a Citrix recomenda que você atualize todos os componentes e VDAs para que possa acessar todos os recursos novos e aprimorados em sua edição e versão.

Por exemplo, embora você possa usar VDAs atuais em implantações que contêm versões anteriores do Controller, novos recursos na versão atual podem não estar disponíveis. Problemas de registro de VDA também podem ocorrer ao usar versões não atuais.

Em alguns ambientes, talvez você não consiga fazer upgrade de todos os VDAs para a versão mais atual. Nesse caso, ao criar um catálogo de máquinas, você pode especificar a versão do VDA instalada nas máquinas. (Isso é chamado de nível funcional.) Por padrão, essa configuração especifica a versão mínima recomendada do VDA. O valor padrão é suficiente para a maioria das implantações. Considere alterar a configuração para uma versão anterior somente se o catálogo contiver VDAs anteriores ao padrão. Não é recomendável misturar versões de VDA em um catálogo de máquinas.

Se um catálogo for criado com a configuração padrão de versão mínima do VDA, e uma ou mais máquinas tiverem um VDA anterior à versão padrão, essas máquinas não poderão se registrar no Controller e não funcionarão.

Para obter mais informações, consulte Versões de VDA e níveis funcionais.

### Vários sites com versões diferentes

Quando seu ambiente contém sites com diferentes versões de produto (por exemplo, um site XenDesktop 7.18 e um site Citrix Virtual Apps and Desktops 1909), a Citrix recomenda usar o StoreFront para agregar aplicativos e desktops de diferentes versões de produto. Para obter detalhes, consulte a documentação do StoreFront.

Em um ambiente misto, continue usando as versões do Studio e do Director para cada lançamento, mas certifique-se de que as diferentes versões estejam instaladas em máquinas separadas.

## Sistemas operacionais anteriores

Digamos que você instalou uma versão anterior de um componente em uma máquina que estava executando uma versão de sistema operacional (SO) compatível. Agora, você deseja usar uma versão mais recente do componente, mas esse SO não é mais compatível com a versão atual do componente.

Por exemplo, suponha que você instalou um VDA de servidor em uma máquina Windows Server 2008 R2. Agora você deseja fazer upgrade desse VDA para a versão atual, mas o Windows Server 2008 R2 não é compatível com a versão atual para a qual você está fazendo upgrade.

Se você tentar instalar ou fazer upgrade de 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 ao upgrade das versões Current Release e Long Term Service Release. (Não afeta a aplicação de CUs a uma versão LTSR.)

Siga os links para saber quais SOs são suportados:

- Citrix Virtual Apps and Desktops (Versão Atual):
  - Delivery Controller, Studio, Director, VDAs, Universal Print Server(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html)
  - Serviço de Autenticação Federada(/pt-br/federated-authentication-service/current-release/system-requirements.html)
  - Para StoreFront, Self-Service Password Reset e Session Recording, consulte o artigo de requisitos do sistema para a versão atual.
- Para LTSRs, consulte as listas de componentes para sua versão LTSR e CU. (Selecione sua versão LTSR na página principal de documentação do produto Citrix Virtual Apps and Desktops.)

### Sistemas operacionais inválidos

A tabela a seguir lista os sistemas operacionais anteriores que não são válidos para instalar/atualizar componentes na versão atual. Ela indica a versão mais recente de componente válida suportada para cada SO listado e a versão do componente quando a instalação e a atualização se tornaram inválidas.

Os sistemas operacionais na tabela incluem service packs e atualizações.

**Sistema operacional | Componente/recurso | Versão válida mais recente | Instalação/ atualização não possível a partir da versão**

| | | | |
|---|---|---|---|
| Windows 7 e Windows 8 | VDA | 7.15 LTSR | 7.16 |
| Windows 7 e Windows 8 | Outros componentes do instalador | 7.17 | 7.18 |
| Versões do Windows 10 anteriores a 1607 | VDA | 7.15 LTSR | 7.16 |
| Versão do Windows 10 x86 | VDA | 1906.2.0 | 1909 |
| Windows Server 2008 R2 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2008 R2 | Outros componentes do instalador | 7.17 | 7.18 |
| Windows Server 2012 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2012 | Outros componentes do instalador | 7.17 | 7.18 |
| Windows Server 2012 R2 | Outros componentes do instalador * | 1912 LTSR | 2003 |
| Windows Server 2012 R2 | Server VDI | 7.15 LTSR | 7.16 |

Windows XP e Windows Vista não são válidos para nenhum componente ou tecnologia 7.x.

* Aplica-se a Delivery Controller, Studio, Director e VDAs.

### O que você pode fazer

Você tem opções. Você pode:

- Continuar com o SO atual
- Reimagear ou atualizar a máquina

- Adicionar novas máquinas e depois remover as máquinas antigas

**Continuar com o sistema operacional atual**

Esses métodos são viáveis para VDAs. Se você quiser continuar usando máquinas com o sistema operacional anterior, você pode escolher uma das seguintes opções:

- Continuar usando a versão do componente instalada.
- Baixe a versão mais recente válida do componente e, em seguida, atualize o componente para essa versão. (Isso pressupõe que a versão mais recente válida do componente ainda não esteja instalada.)

Por exemplo, você tem um VDA 7.14 em uma máquina Windows 7 SP1. A versão VDA válida mais recente em máquinas com SO Windows 7 é XenApp e XenDesktop 7.15 LTSR. Você pode continuar usando o 7.14 ou baixar um VDA 7.15 LTSR e, em seguida, atualizar seu VDA para essa versão. Essas versões VDA anteriores funcionam em implantações que contêm Delivery Controllers com versões mais recentes. Por exemplo, um VDA 7.15 LTSR pode se conectar a um Controller do Citrix Virtual Apps and Desktops 7 1808.

**Reimage ou atualize a máquina**

Esses métodos são viáveis para VDAs e outras máquinas que não possuem componentes principais (como Delivery Controllers) instalados. Escolha uma das seguintes opções:

- Depois de desativar a máquina (ativando o modo de manutenção e permitindo que todas as sessões sejam fechadas), você pode reimaginá-la para uma versão de SO Windows compatível e, em seguida, instalar a versão mais recente do componente.
- Para atualizar o SO em uma máquina VDA sem reimaginá-la, você deve primeiro instalar a versão do VDA compatível com o SO para o qual você está atualizando ou atualizar o VDA após atualizar o SO. Caso contrário, o software Citrix não será compatível. Você pode atualizar para as seguintes versões mínimas de SO ao realizar uma atualização in-loco sem desinstalar o VDA:
  - Windows 11 com Atualização Cumulativa de 2023-07 para Windows 11 (KB5028185) ou posterior instalado (compilação 22621.1992 ou posterior).
  - Windows 10 com Atualização Dinâmica de 2023-07 para Windows 10 (KB5028311) instalado.
- Se a versão do Windows para a qual você planeja atualizar não estiver alinhada com a diretriz mencionada, você deve desinstalar o VDA antes de atualizar o SO e, em seguida, instalar uma versão VDA compatível após a conclusão da atualização do SO.

### Adicionar novas máquinas e depois remover as máquinas antigas

Este método é viável se você precisar atualizar o SO em máquinas que contêm um Delivery Controller™ ou outro componente principal.

A Citrix recomenda que todos os Controllers em um site tenham o mesmo SO. A seguinte sequência de atualização minimiza o intervalo em que diferentes Controllers têm SOs diferentes.

1. Crie um 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 Controller 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 Controllers em Delivery Controllers.

## Preparação

Antes de iniciar uma atualização, revise as seguintes informações e conclua as tarefas necessárias.

> **Observação:**
>
> Embora a atualização de VDAs ocorra mais tarde na sequência de atualização, é uma boa ideia escolher um instalador e revisar o procedimento antes de iniciar a atualização, para que você saiba o que esperar.

### Escolha um instalador e interface

Use o instalador completo do produto a partir da ISO do produto para atualizar os componentes. Você pode atualizar VDAs usando o instalador completo do produto ou um dos instaladores VDA autônomos. Todos os instaladores oferecem interfaces gráficas e de linha de comando.

Para obter mais informações, consulte Instaladores.

**Especificidades da instalação:** Depois de concluir qualquer trabalho de preparação e estiver pronto para iniciar o instalador, o artigo de instalação mostra o que você verá (se estiver usando a interface gráfica) ou o que digitar (se estiver usando a interface de linha de comando).

- Instalar/atualizar componentes principais usando a interface gráfica
- Instalar/atualizar componentes principais usando a linha de comando
- Instalar/atualizar VDAs usando a interface gráfica
- Instalar/atualizar VDAs usando a linha de comando

Se você instalou originalmente um VDA de sessão única com o instalador `VDAWorkstationCoreSetup.exe`, a Citrix recomenda usar esse instalador para atualizá-lo. Se você usar o instalador VDA de produto completo ou o instalador `VDAWorkstationSetup.exe` para atualizar o VDA, os componentes que foram originalmente excluídos podem ser instalados, a menos que você os omita/exclua expressamente da atualização.

Ao atualizar um VDA para a versão atual, uma reinicialização da máquina ocorre durante o processo de atualização. (Este requisito começou com a versão 7.17.) Isso não pode ser evitado. A atualização é retomada automaticamente após a reinicialização (a menos que você especifique `/noresume` na linha de comando).

### Ações do banco de dados

Faça backup dos bancos de dados do site, de monitoramento e de registro de configuração. Siga as instruções em CTX135207. Se algum problema for descoberto após a atualização, você poderá restaurar o backup.

Para obter informações sobre como atualizar versões do SQL Server que não são mais suportadas, consulte Verificação de versão do SQL Server. (Isso se refere ao SQL Server que é usado para os bancos de dados de site, monitor e registro de configuração.)

O Microsoft SQL Server Express LocalDB é instalado automaticamente, para uso com o Local Host Cache. Se você precisar substituir uma versão anterior, a nova versão deve ser o SQL Server Express LocalDB 2019. Para obter detalhes sobre como substituir o SQL Server Express LocalDB pela nova versão após a atualização dos componentes e do site, consulte Substituir SQL Server Express LocalDB.

### Certifique-se de que sua licença Citrix esteja atualizada

Para uma visão abrangente do gerenciamento de licenciamento Citrix, consulte Ativar, atualizar e gerenciar licenças Citrix.

Você pode usar o instalador de produto completo para atualizar o License Server. Ou, você pode baixar e atualizar os componentes de licença separadamente. Consulte Atualizar.

Antes de atualizar, certifique-se de que a data do seu Customer Success Services / Software Maintenance / Subscription Advantage seja válida para a nova versão do produto. A data deve ser de pelo menos 15/11/2021.

### Certifique-se de que seu Citrix License Server seja compatível

Certifique-se de que seu Citrix License Server seja compatível com a nova versão. Existem duas maneiras de fazer isso:

- Antes de atualizar quaisquer outros componentes Citrix, execute o instalador `XenDesktopServerSetup.exe` do layout ISO na máquina que contém um Delivery Controller. Se houver problemas de incompatibilidade, o instalador os relatará com as etapas recomendadas para resolvê-los.
- No diretório `XenDesktop Setup` na mídia de instalação, execute o comando: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. A exibição indica se o License Server é compatível. Se o License Server for incompatível, atualize o servidor de licenças.

### Faça backup de quaisquer modificações do StoreFront

Antes de iniciar uma atualização, se você fez modificações em arquivos em `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como *default.ica* e *usernamepassword.tfrm*, faça backup deles para cada loja. Após a atualização, você pode restaurá-los para restabelecer suas modificações.

### Fechar aplicativos e consoles

Antes de iniciar uma atualização, feche todos os programas que possam causar bloqueios de arquivo, incluindo consoles de administração e sessões do PowerShell.

Reiniciar a máquina garante que quaisquer bloqueios de arquivo sejam liberados e que não haja atualizações pendentes do Windows.

Antes de iniciar uma atualização, pare e desative quaisquer serviços de agente de monitoramento de terceiros.

### Certifique-se de ter as permissões adequadas

Além de ser um usuário de domínio, você deve ser um administrador local nas máquinas onde está atualizando os componentes do produto.

O banco de dados do site e o site podem ser atualizados automaticamente ou manualmente. Para uma atualização automática do banco de dados, as permissões do usuário do Studio devem incluir a capacidade de atualizar o esquema do banco de dados do SQL Server (por exemplo, a função de banco de dados `db_securityadmin` ou `db_owner`). Para obter detalhes, consulte Bancos de dados.

Se o usuário do Studio não tiver essas permissões, iniciar uma atualização manual do banco de dados gera scripts. O usuário do Studio executa alguns dos scripts a partir do Studio. O administrador do banco de dados executa outros scripts, usando uma ferramenta como o SQL Server Management Studio.

### Outras tarefas de preparação

- Faça backup de modelos e atualize hipervisores, se necessário
- Conclua quaisquer outras tarefas de preparação ditadas pelo seu plano de continuidade de negócios.

## Testes preliminares do site

Ao atualizar os Delivery Controllers e um site, testes preliminares do site são executados antes do início da atualização real. Esses testes verificam:

- O banco de dados do site pode ser acessado e foi feito backup
- As conexões com os serviços essenciais do Citrix estão funcionando corretamente
- O endereço do Citrix License Server está disponível
- O banco de dados de log de configuração pode ser acessado
- Certifique-se de ter a Licença de Direitos Híbridos se quiser adicionar conexões de host de nuvem pública (por exemplo, AWS). Caso contrário, o teste preliminar do site pausa ou para, e uma mensagem explicativa aparece.

Após a execução dos testes, você pode visualizar um relatório dos resultados. Você pode então corrigir quaisquer problemas detectados e executar os testes novamente. A falha em executar os testes preliminares do site e, em seguida, resolver quaisquer problemas pode afetar o funcionamento do seu site.

O relatório contendo os resultados do teste é um arquivo HTML (`PreliminarySiteTestResult.html`) no mesmo diretório dos logs de instalação. Esse arquivo é criado se não existir. Se o arquivo existir, seu conteúdo será sobrescrito.

### Executar os testes

- Ao usar a interface gráfica do instalador para atualizar, o assistente inclui uma página onde você pode iniciar os testes e, em seguida, exibir o relatório. Depois que os testes forem executados e você tiver visualizado o relatório e resolvido quaisquer problemas encontrados, você poderá executar os testes novamente. Quando os testes forem concluídos com sucesso, clique em Avançar para continuar com o assistente.
- Ao usar a interface de linha de comando para atualizar, os testes são executados automaticamente. Por padrão, se um teste falhar, a atualização não é realizada. Depois de visualizar o relatório e resolver os problemas, execute o comando novamente.

A Citrix recomenda sempre executar os testes preliminares do site e, em seguida, resolver quaisquer problemas antes de continuar a atualização do Controller e do site. O benefício potencial vale bem os poucos momentos para executar os testes. No entanto, você pode substituir esta ação recomendada.

- Ao atualizar com a interface gráfica, você pode optar por pular os testes e continuar com a atualização.
- Ao atualizar pela linha de comando, você não pode pular os testes. Por padrão, um teste de site com falha faz com que o instalador falhe, sem realizar a atualização. Na maioria dos casos, se você incluir a opção `/ignore_site_test_failure`, quaisquer falhas de teste são ignoradas e a atualização prossegue. (Consulte Verificação da versão do SQL Server para exceções.)

### Ao atualizar vários Controllers

Ao iniciar uma atualização em um Controller e, em seguida, iniciar uma atualização de outro Controller no mesmo site (antes que a primeira atualização seja concluída):

- Se os testes preliminares do site tiverem sido concluídos no primeiro Controller, a página de testes preliminares do site não aparecerá no assistente no outro Controller.
- Se os testes no primeiro Controller estiverem em andamento quando você iniciar a atualização no outro Controller, a página de testes do site aparecerá no assistente no outro Controller. No entanto, se os testes no primeiro Controller terminarem, apenas os resultados dos testes do primeiro Controller serão mantidos.

### Falhas de teste não relacionadas à integridade do site

- Se os testes preliminares do site falharem devido a memória insuficiente, disponibilize mais memória e execute os testes novamente.

- Se você tiver permissão para atualizar, mas não para executar testes de site, os testes preliminares do site falharão. Para resolver isso, execute o instalador novamente com uma conta de usuário que tenha permissão para executar os testes.

## Verificação da versão do SQL Server

Uma implantação bem-sucedida do Citrix Virtual Apps and Desktops requer uma versão compatível do Microsoft SQL Server para os bancos de dados de site, monitor e registro de configuração. A atualização de uma implantação Citrix com uma versão do SQL Server que não é mais compatível pode resultar em problemas de funcionalidade, e o site não será compatível.

Para saber quais versões do SQL Server são compatíveis com a versão do Citrix para a qual você está atualizando, consulte o artigo Requisitos do sistema para essa versão.

Ao atualizar um Controller, o instalador Citrix verifica a versão do SQL Server atualmente instalada usada para os bancos de dados de site, monitor e registro de configuração.

- Se a verificação determinar que a versão do SQL Server atualmente instalada não é uma versão compatível na versão do Citrix para a qual você está fazendo upgrade:
  - Interface gráfica: A atualização é interrompida com uma mensagem. Clique em **Entendi** e depois em **Cancelar** para fechar o instalador Citrix. (Você não pode continuar com a atualização.)
  - Interface de linha de comando: o comando falha (mesmo que você tenha incluído a opção `/ignore_db_check_failure` com o comando).

  Faça upgrade da versão do SQL Server e, em seguida, inicie o upgrade do Citrix novamente.
- Se a verificação não conseguir determinar qual versão do SQL Server está atualmente instalada, verifique se a sua versão atualmente instalada é compatível com a versão para a qual você está atualizando (Requisitos do sistema).
  - Interface gráfica: O upgrade é interrompido com uma mensagem.
    - Se a versão do SQL Server atualmente instalada for compatível, clique em **Entendi** para fechar a mensagem e, em seguida, clique em **Avançar** para continuar com a atualização do Citrix.
    - Se a versão do SQL Server atualmente instalada não for suportada, clique em **Entendi** para fechar a mensagem e, em seguida, clique em **Cancelar** para encerrar a atualização do Citrix. Atualize seu SQL Server para uma versão suportada e, em seguida, inicie a atualização do Citrix novamente.

- Interface de linha de comando: O comando falha com uma mensagem. Após fechar a mensagem:
  - Se a versão do SQL Server atualmente instalada for suportada, execute o comando novamente com a opção `/ignore_db_check_failure`.
  - Se a versão do SQL Server atualmente instalada não for suportada, atualize seu SQL Server para uma versão suportada. Execute o comando novamente para iniciar a atualização do Citrix.

### Atualizando o SQL Server

Se você configurar novos servidores SQL Server e migrar o banco de dados do site, as cadeias de conexão deverão ser atualizadas.

Se o site usa atualmente o SQL Server Express para o banco de dados do site (que o Citrix instalou automaticamente durante a criação do site):

1. Instale a versão mais recente do SQL Server Express.
2. Desanexe o banco de dados.
3. Anexe o banco de dados ao novo SQL Server Express.
4. Migre as cadeias de conexão.

Para obter mais informações, consulte Configurando cadeias de conexão e a documentação do produto Microsoft SQL Server.

## Substituir SQL Server Express LocalDB

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

O Citrix não atualiza automaticamente o SQL Server Express LocalDB. Para atualizar a versão do SQL Server Express LocalDB, siga as orientações nesta seção.

- Ao atualizar os Delivery Controllers para o Citrix Virtual Apps and Desktops versão 2203 LTSR ou versões posteriores, a versão suportada é SQL Server Express LocalDB 2019 ou SQL Server Express LocalDB 2022.

O que você precisa:

- A mídia de instalação do Citrix Virtual Apps and Desktops.

- A ferramenta PsExec da caixa de ferramentas do Windows Sysinternals.

Procedimento:

1. Conclua a atualização dos componentes, bancos de dados e site do Citrix Virtual Apps and Desktops. (Essas atualizações de banco de dados afetam os bancos de dados de site, monitoramento e registro de configuração. Elas não afetam o banco de dados Local Host Cache que usa SQL Server Express LocalDB.)
2. Faça logon no Delivery Controller, onde você gostaria de atualizar o SQL Server Express LocalDB.
3. Baixe o PsExec da Microsoft e coloque-o em um local de fácil acesso nesse Delivery Controller, como C:\Temp.
4. Pare o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
5. Abra o Prompt de Comando no Delivery Controller, navegar até o local com o PsExec (exemplo, `C:\Temp`), e então execute o seguinte comando para elevar o prompt de comando com a conta Network Service:

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. Execute `whoami` para confirmar que o prompt de comando está sendo executado como a conta Network Service. Você deve obter a seguinte saída: `nt authority\networkservice`.
7. Use o prompt de comando para navegar até a instância do SQL LocalDB:
   - Se estiver atualizando do SQL LocalDB 2014:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2017:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2019:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. Pare e exclua a instância do SQL LocalDB: `CitrixHA`.

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Remova os seguintes arquivos do Delivery Controller:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. Desinstale seu SQL LocalDB SQL Server Express existente do Delivery Controller usando o recurso nativo do Windows para remover programas.
11. Reinicie o Delivery Controller após a conclusão da desinstalação.
12. Pare o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
13. Monte a mídia de instalação do Citrix Virtual Apps and Desktops no seu Delivery Controller.
14. Instale o SQL Server Express LocalDB 2022 como administrador no Delivery Controller.
    a. Use o arquivo `sqllocaldb.msi` na pasta `Support > SQLLocalDB` da mídia de instalação do Citrix Virtual Apps and Desktops. Por exemplo, se a mídia de instalação estiver montada na letra `E drive`, o arquivo pode ser encontrado em `E:\Support\SQLLocalDB\sqllocaldb.msi`. É necessário reiniciar para concluir a instalação.
    b. O novo SQL LocalDB deve estar em `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`.
15. Inicie o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.

16. No Prompt de Comando do Delivery Controller, navegar até `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` e execute `SqlLocalDB i` para confirmar que a instância CitrixHA foi criada. O `CitrixHA` deve ser incluído na lista de instâncias retornadas.

    > **Nota:**
    >
    > Pode levar até 15 minutos para que o banco de dados CitrixHA seja criado após o início do Serviço de Alta Disponibilidade do Citrix.

17. Certifique-se de que os arquivos do banco de dados do Cache do Host Local sejam criados para confirmar que o Serviço de Alta Disponibilidade (broker secundário) pode assumir o controle, se necessário.

    a. No Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.

    b. Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.

18. Repita as etapas nos Delivery Controllers restantes.

# Suporte a Proxy para o Agente de Atualização VDA

O suporte a proxy para o Agente de Atualização VDA foi adicionado no VDA 2311.

O Agente de Atualização VDA do VDA 2311, ou seja, Versão: 7.40, pode reconhecer e enviar tráfego através do Proxy.

O Agente de Atualização VDA (VUA) suporta Proxy na forma de Hostname:Porta (IP:Porta) e arquivo PAC.

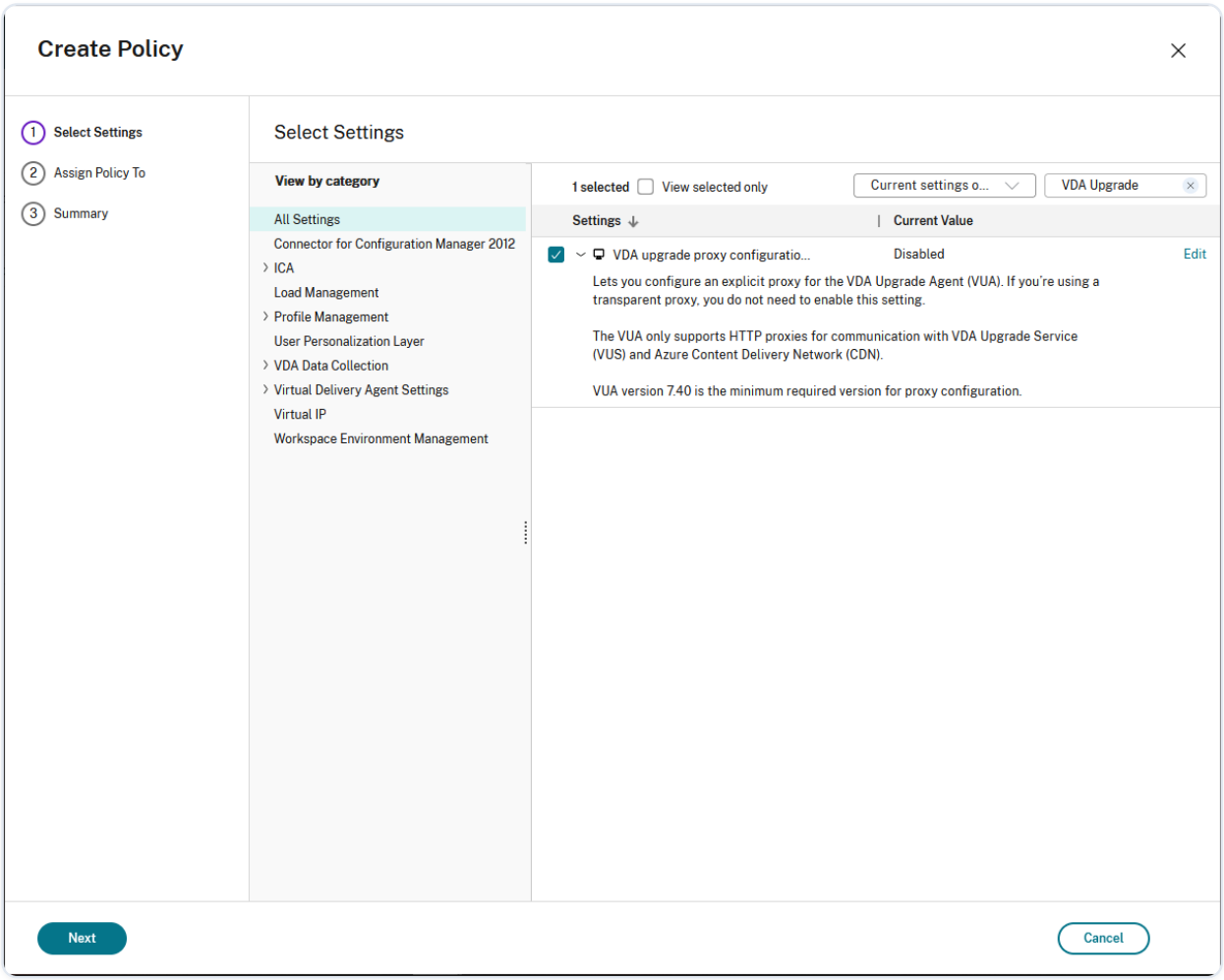
Apenas proxies HTTP são suportados. A descriptografia e inspeção de pacotes não são suportadas.

A autenticação de proxy não é suportada. SOCKS5 não é suportado.

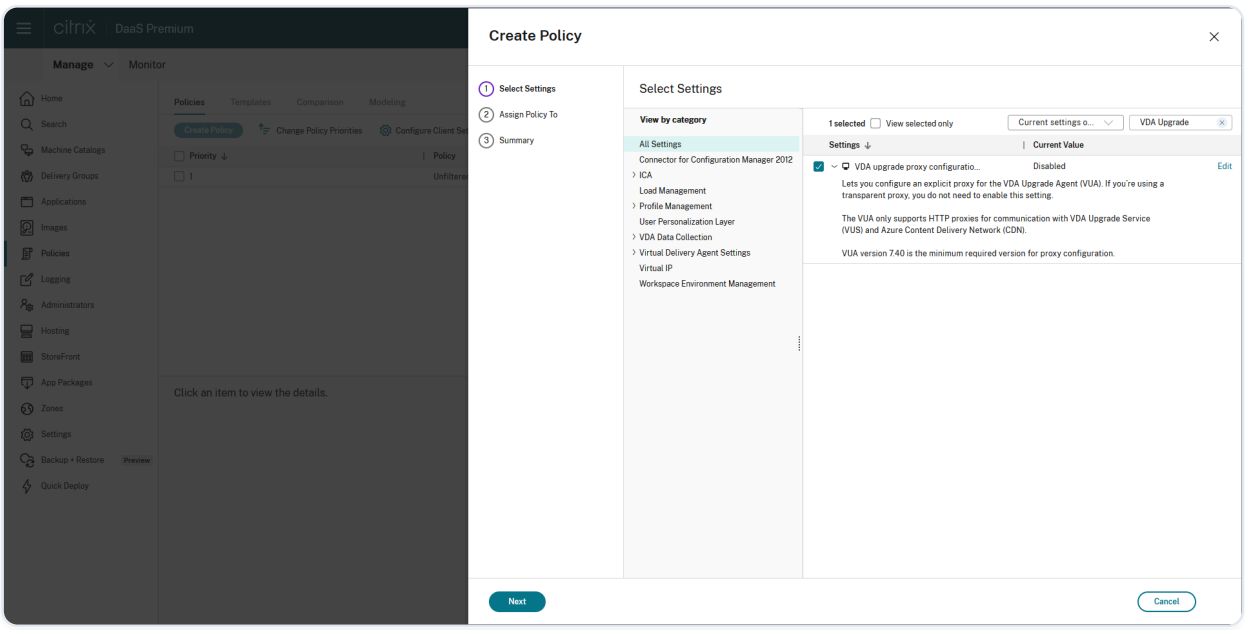
## Configurando o Proxy do Agente de Atualização VDA

### O Proxy do Agente de Atualização VDA pode ser configurado de 2 maneiras

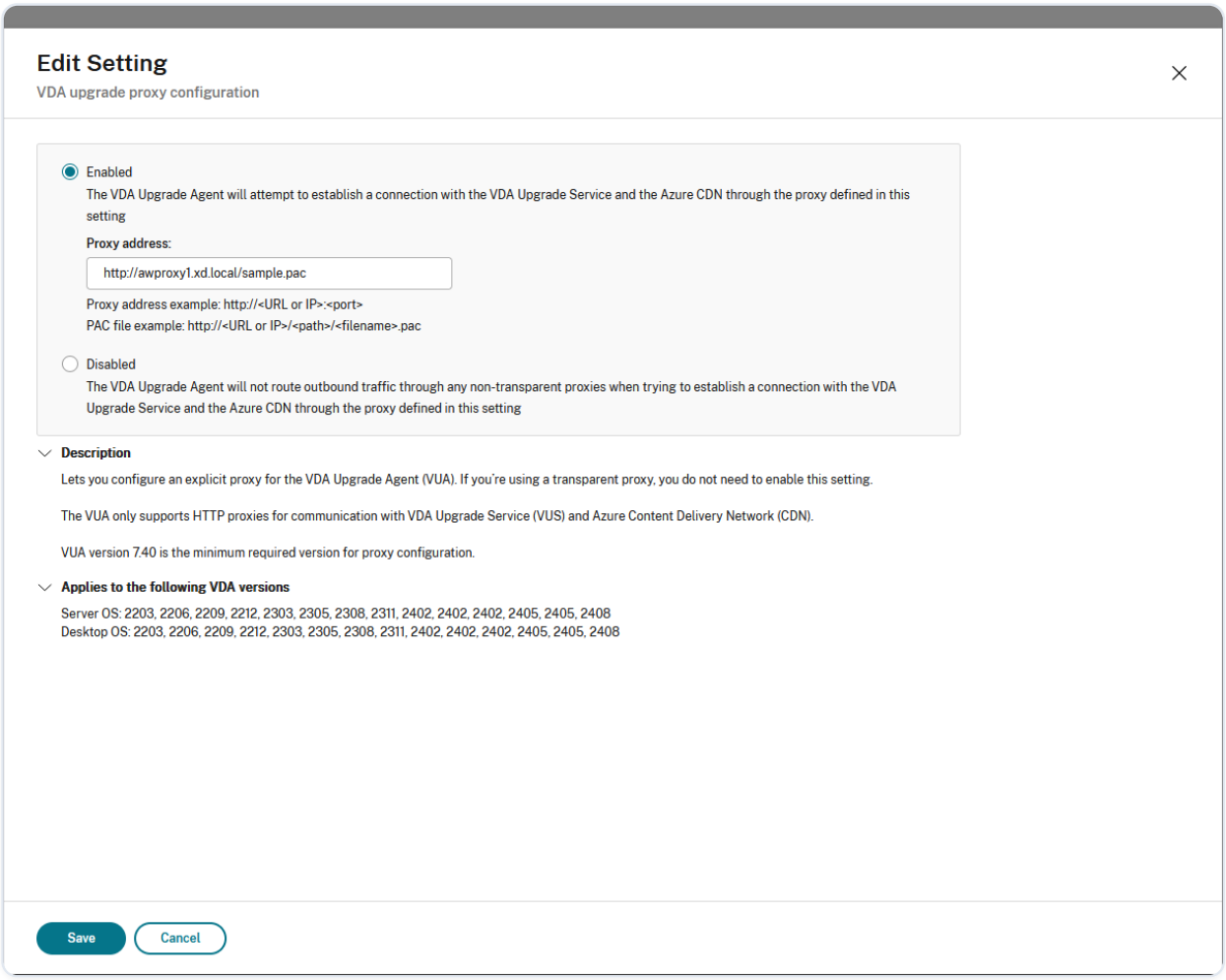
1. **Configurando a Política do Agente de Atualização VDA** usando a **Política do Webstudio**.



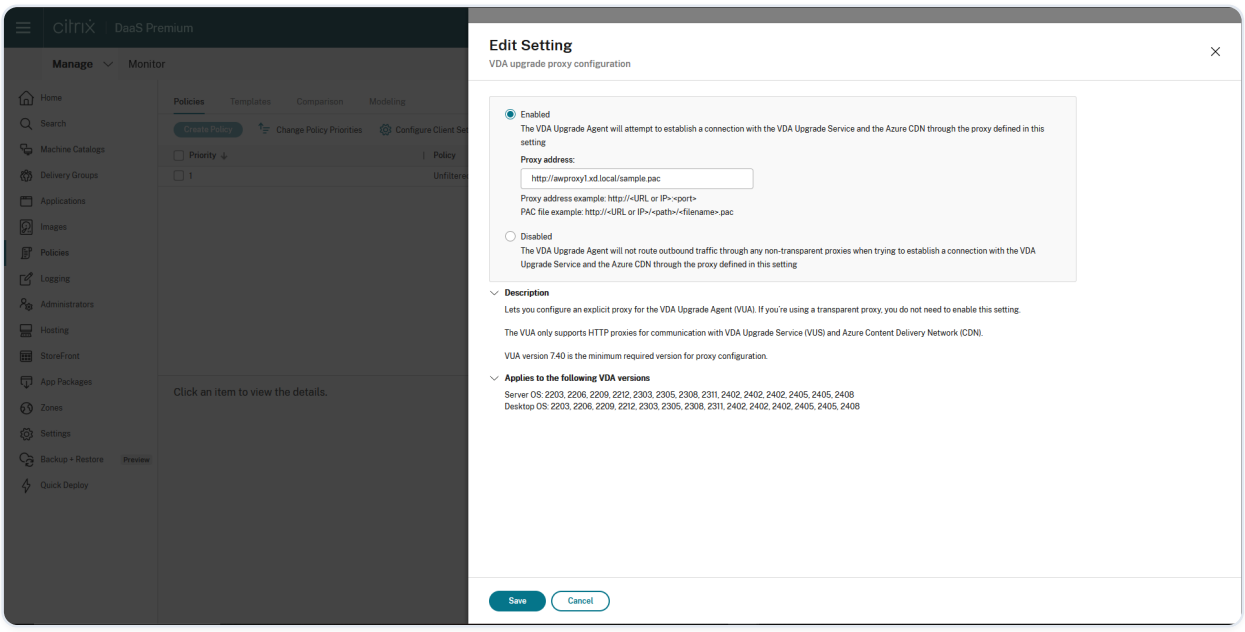

2. Selecione **Configuração de proxy de atualização VDA** em **Configurações** na página **Criar Política**.




3. Habilite a configuração. Por padrão, a configuração está desabilitada.




4. Configurando o Agente de Atualização VDA usando a Chave de Registro.




A chave do registro é definida como Meta-Installer durante a instalação do VDA.

Registro:

**Chave:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

**Tipo de valor:** String

**Nome do valor:** ProxySettings

**Dados do valor:** Endereço do proxy ou caminho para o arquivo pac.

**Por exemplo:**

a. Endereço do proxy: `http://<URL or IP>:<port>`
b. Arquivo pac: `http://<URL or IP>/<path/<filename>.pac`

# Fazer backup ou migrar sua configuração

Este recurso ajuda você a fazer backup de suas configurações DaaS. Os backups facilitam o processo de migração das configurações de um site em nuvem para outro. Também facilita a recuperação imediata de um site em caso de emergência. Você pode usar os seguintes métodos para fazer backups:

1. Backup + Restauração
    a. Integrado com o WebStudio.
2. Ferramenta de Configuração Automatizada (ACT)
    a. Ferramenta baseada em Powershell. Instale a ferramenta para usá-la.

Os backups podem ser usados para:

1. Restauração
2. Migração

A Citrix® recomenda as seguintes ferramentas para os cenários descritos.

## Backup

| AMBIENTE | CASO DE USO | FERRAMENTA RECOMENDADA | CONSIDERAÇÕES ESPECIAIS | LINK |
|---|---|---|---|---|
| DaaS | Backups sob demanda e agendados | Backup + Restauração | A Citrix mantém o backup e o usuário pode | Backup + Restauração no Studio |

| AMBIENTE | CASO DE USO | FERRAMENTA RECOMENDADA | CONSIDERAÇÕES ESPECIAIS | LINK |
|---|---|---|---|---|
| | | | baixá-lo se necessário | |
| No local | Backups sob demanda | ACT | O usuário mantém o backup | Backup e Restauração usando a Ferramenta de Configuração Automatizada |

## Migração

| AMBIENTE | CASO DE USO | FERRAMENTA RECOMENDADA | CONSIDERAÇÕES ESPECIAIS | LINK |
|---|---|---|---|---|
| No local para a nuvem | Migrar um site local para DaaS | ACT | | Migrar do local para a nuvem |
| | Consolidar vários sites locais em um site DaaS | ACT | Fusão de sites | Mesclar vários sites locais em um único site na nuvem |
| No local para no local | Migrar um site local para outro site local | ACT | | Guia de POC:Ferramenta de Configuração Automatizada - Migração local para local |
| | Consolidar vários sites locais em outro site local | ACT | Fusão de sites | Guia de POC:Ferramenta de Configuração Automatizada Migração local para local |

| AMBIENTE | CASO DE USO | FERRAMENTA RECOMENDADA | CONSIDERAÇÕES ESPECIAIS | LINK |
|---|---|---|---|---|
| | | | | Mesclar vários sites locais em um único site na nuvem |
| Nuvem para nuvem | Migrar um site DaaS para outro site DaaS | ACT | | Migrar da nuvem para a nuvem(/pt-br/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration) |
| Consolidar vários sites DaaS em um único site DaaS | ACT | Fusão de sites | | Migrar da nuvem para a nuvem(/pt-br/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration) |
| | | | | Migrar vários sites locais para um único site na nuvem(/pt-br/citrix-daas/migrate/multi-site-merge.html) |

# Seguro

O Citrix Virtual Apps and Desktops™ oferece uma solução segura por design que permite adaptar seu ambiente às suas necessidades de segurança.

Uma preocupação de segurança que a TI enfrenta com trabalhadores móveis é a perda ou roubo de dados. Ao hospedar aplicativos e desktops, o Citrix Virtual Apps and Desktops separa com segurança dados sensíveis e propriedade intelectual de dispositivos de ponto de extremidade, mantendo todos os dados em um data center. Quando as políticas são habilitadas para permitir a transferência de dados, todos os dados são criptografados.

Os data centers do Citrix Virtual Apps and Desktops também facilitam a resposta a incidentes com um serviço centralizado de monitoramento e gerenciamento. O Director permite que a TI monitore e analise os dados que estão sendo acessados na rede, e o Studio permite que a TI corrija e remedie a maioria das vulnerabilidades no data center, em vez de resolver os problemas localmente em cada dispositivo do usuário final.

O Citrix Virtual Apps and Desktops também simplifica auditorias e conformidade regulatória, pois os investigadores podem usar um registro de auditoria centralizado para determinar quem acessou quais aplicativos e dados. O Director coleta dados históricos sobre atualizações do sistema e uso de dados do usuário acessando o Log de Configuração e a API OData.

A administração delegada permite configurar funções de administrador para controlar o acesso ao Citrix Virtual Apps and Desktops em um nível granular. Isso permite flexibilidade em sua organização para conceder a certos administradores acesso total a tarefas, operações e escopos, enquanto outros administradores têm acesso limitado.

O Citrix Virtual Apps and Desktops oferece aos administradores controle granular sobre os usuários, aplicando políticas em diferentes níveis da rede - do nível local ao nível da Unidade Organizacional. Esse controle de políticas determina se um usuário, dispositivo ou grupos de usuários e dispositivos podem se conectar, imprimir, copiar/colar ou mapear unidades locais, o que pode minimizar preocupações de segurança com trabalhadores temporários de terceiros. Os administradores também podem usar o recurso Bloqueio de Área de Trabalho para que os usuários finais possam usar apenas a área de trabalho virtual, impedindo qualquer acesso ao sistema operacional local do dispositivo do usuário final.

Os administradores podem aumentar a segurança no Citrix Virtual Apps ou Citrix Virtual Desktops configurando o Site para usar o protocolo Transport Layer Security (TLS) do Controller ou entre usuários finais e Virtual Delivery Agents (VDA). O protocolo também pode ser habilitado em um Site para fornecer autenticação de servidor, criptografia de fluxo de dados e verificações de integridade de mensagens para uma conexão TCP/IP.

O Citrix Virtual Apps and Desktops também suporta autenticação multifator para Windows ou um aplicativo específico. A autenticação multifator também pode ser usada para gerenciar todos os recursos entregues pelo Citrix Virtual Apps and Desktops. Esses métodos incluem:

- Tokens
- Cartões inteligentes
- RADIUS
- Kerberos
- Biometria

O Citrix Virtual Desktops pode ser integrado com muitas soluções de segurança de terceiros, desde gerenciamento de identidade até software antivírus. Uma lista de produtos suportados pode ser encontrada em `<http://www.citrix.com/ready>`.

Versões selecionadas do Citrix Virtual Apps and Desktops são certificadas para o padrão Common Criteria. Para uma lista desses padrões, acesse `<https://www.commoncriteriaportal.org/cc/>`.

## Serviço de Autenticação Federada

O Citrix Federated Authentication Service (FAS) permite o logon único (SSO) em desktops virtuais e aplicativos Citrix em ambientes onde os usuários autenticar por meio de provedores de identidade modernos, como SAML ou OpenID Connect (OIDC), que não fornecem uma senha do Windows, garantindo acesso contínuo aos hosts de sessão unidos a um domínio do Active Directory.

Para obter mais informações sobre como proteger sua implantação com o Serviço de Autenticação Federada, consulte a documentação do Serviço de Autenticação Federada em seu próprio documento.

# Autenticação FIDO2 e WebAuthn

## Autorização local e autenticação virtual usando FIDO2 e WebAuthn

Os usuários podem autenticar em aplicativos que utilizam FIDO2 ou WebAuthn em sua sessão virtual usando chaves de segurança FIDO2 e dispositivos biométricos integrados com TPM 2.0 e Windows Hello.

Para obter mais informações sobre FIDO2, consulte FIDO2: WebAuthn & CTAP.

Para obter informações sobre como usar esse recurso, consulte Redirecionamento FIDO2.

**NOTA**

Observe que esse recurso não oferece suporte ao login na sessão virtual usando WebAuthn ou FIDO2. Esse recurso permite apenas o uso desses métodos de autenticação em aplicativos dentro da sessão virtual.

Este recurso não é compatível em cenários de salto duplo (double-hop).

## Matriz de compatibilidade

| SISTEMA OPERACIONAL DO HOST DA SESSÃO | AUTENTICAÇÃO DE APLICATIVO WEB | AUTENTICAÇÃO DE APLICATIVO UWP |
|---|---|---|
| Windows Server 2016 | Compatível via redirecionamento USB | Não compatível |
| Windows Server 2019 | Suportado | Não suportado |
| Windows Server 2022 | Suportado | Suportado |
| Windows 10 | Suportado | Suportado |
| Windows 11 | Suportado | Suportado |

Para obter informações adicionais, revise os requisitos abaixo.

# Autenticação de aplicativo web

## Requisitos

A seguir estão os requisitos para usar a autenticação FIDO2 e WebAuthn com aplicativos web:

### Plano de controle Citrix®

- Citrix Virtual Apps and Desktops™ 2009 ou posterior

### Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2019 ou posterior
- VDA
  - Windows: versão 2009 ou posterior

### Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux
- Aplicativo Workspace
  - Windows: versão 2009.1 ou posterior
  - Linux: 2303 ou posterior

### Requisitos do navegador web

- Navegadores de 64 bits
- Navegadores de 32 bits (Citrix Virtual Apps and Desktops™ 2402 CU2 e posterior)

> **NOTA**
>
> Ao usar um navegador baseado em Chromium dentro de sua sessão de aplicativo ou desktop virtual, o registro da chave FIDO2 não funciona se o navegador estiver executando a versão 147 do Chromium ou mais recente. A atualização para a versão 2503 do VDA ou mais recente resolve esse problema. Alternativamente, como solução alternativa, você pode

> desabilitar o redirecionamento FIDO2 e usar o redirecionamento USB para redirecionar a chave FIDO2 para a sessão. Para detalhes, consulte Redirecionamento USB.

#### Métodos de autenticação suportados

- Chave de Segurança FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial
    - Leitor de impressão digital
  - WebAuthn

## Autenticação de aplicativo UWP

Com o lançamento do Citrix Virtual Apps and Desktops 2112, o Citrix oferece suporte à autenticação WebAuthn e FIDO2 em aplicativos UWP.

Aplicativos como Microsoft Teams, Microsoft Outlook para Office 365 e OneDrive usam um aplicativo UWP para autenticação como um link para o Azure Active Directory. O Citrix agora oferece suporte ao uso do FIDO2 para autenticar esses aplicativos.

### Requisitos

A seguir estão os requisitos para usar a autenticação FIDO2 e WebAuthn com aplicativos UWP:

#### Plano de controle do Citrix

- Citrix Virtual Apps and Desktops 2112 ou posterior

#### Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2022 ou posterior
- VDA
  - Windows: versão 2112 ou posterior

### Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux
- Aplicativo Workspace
  - Windows: versão 2009.1 ou posterior
  - Linux: 2303 ou posterior

### Métodos de autenticação suportados

- Chave de Segurança FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial
    - Leitor de impressão digital
  - WebAuthn

> **Observação:**

> Em cenários onde o redirecionamento FIDO2 não está disponível porque o recurso não é suportado pelo cliente, VDA ou sistema operacional, as chaves FIDO2 baseadas em USB podem ser redirecionadas usando o redirecionamento USB. Também é possível usar o redirecionamento USB para redirecionar chaves FIDO2 baseadas em USB em cenários onde o redirecionamento FIDO2 está disponível. Neste caso, você deve desabilitar o redirecionamento FIDO2 e configurar as regras de redirecionamento USB apropriadas. Consulte a documentação de regras de dispositivo de redirecionamento USB para obter detalhes sobre como configurar chaves FIDO2 usando regras de redirecionamento USB.

## Configuração avançada para aplicativos baseados em msedgewebview2.exe

> **Observação:**

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

> Para empresas que possuem aplicativos web baseados em msedgewebview2.exe, valores de registro adicionais precisam ser adicionados no VDA para que o redirecionamento FIDO2 funcione dentro das sessões HDX -

Anexe o caminho completo do msedgewebview2.exe no valor de registro AllowedProcesses:

- Chave: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- Nome do valor: AllowedProcesses
- Tipo de valor: REG_MULTISZ
- Dados do valor: `<add full path of the msedgewebview2.exe here >`

Para aplicativos de 64 bits, os seguintes valores precisam ser definidos:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: FilePathName
- Tipo de valor: REG_SZ
- Dados do valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: Flag
- Tipo de valor: DWORD
- Dados do valor: 00000002

Para aplicativos de 32 bits, os seguintes valores precisam ser definidos:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: FilePathName
- Tipo de valor: REG_SZ
- Dados do valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: Flag
- Tipo de valor: DWORD
- Dados do valor: 00000002

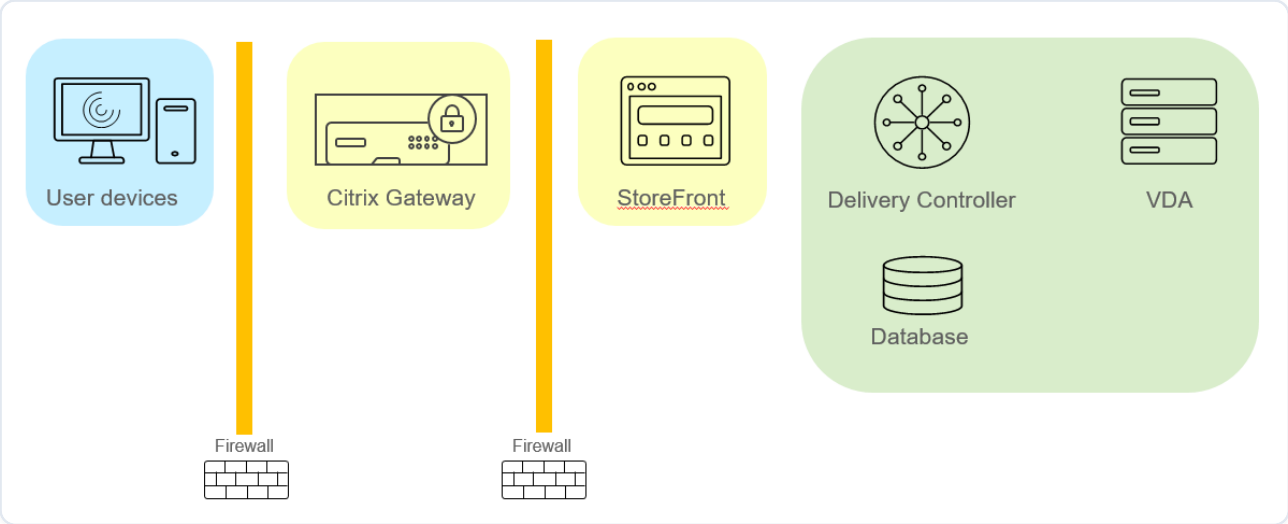
Reinicie o VDA depois de definir os valores do registro para que o redirecionamento FIDO2 seja ativado para aplicativos baseados em msedgewebview2.exe.

# Integrar Citrix Virtual Apps and Desktops™ com Citrix Gateway

Os servidores StoreFront™ são implantados e configurados para gerenciar o acesso a recursos e dados publicados. Para acesso remoto, é recomendável adicionar o Citrix Gateway na frente do StoreFront.

> **Nota:**
>
> Para obter etapas de configuração detalhadas sobre como integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway, consulte a documentação do StoreFront.

> O diagrama a seguir ilustra um exemplo de uma implantação Citrix simplificada que inclui o Citrix Gateway. O Citrix Gateway se comunica com o StoreFront para proteger aplicativos e dados entregues pelo Citrix Virtual Apps and Desktops. Os dispositivos do usuário executam o aplicativo Citrix Workspace™ para criar uma conexão segura e acessar seus aplicativos, desktops e arquivos.




Os usuários fazem login e autenticar usando o Citrix Gateway. O Citrix Gateway é implantado e protegido na DMZ. A autenticação de dois fatores é configurada. Com base nas credenciais do usuário, os usuários recebem os recursos e aplicativos relevantes. Aplicativos e dados estão em servidores apropriados (não mostrados no diagrama). Servidores separados são usados para aplicativos e dados sensíveis à segurança.

# Considerações de segurança e melhores práticas

> **Nota:**

> Sua organização pode precisar atender a padrões de segurança específicos para satisfazer requisitos regulatórios. Este documento não aborda este assunto, pois tais padrões de segurança mudam com o tempo. Para informações atualizadas sobre padrões de segurança e produtos Citrix, consulte `<http://www.citrix.com/security/>`.

## Melhores práticas de segurança

Mantenha todas as máquinas em seu ambiente atualizadas com patches de segurança. Uma vantagem é que você pode usar thin clients como terminais, o que simplifica essa tarefa.

Proteja todas as máquinas em seu ambiente com software antivírus.

Considere usar software anti-malware específico da plataforma.

Ao instalar software, instale nos caminhos padrão fornecidos.

- Se você instalar software em um local de arquivo diferente do caminho padrão fornecido, considere adicionar medidas de segurança adicionais, como permissões restritas, ao seu local de arquivo.

Todas as comunicações de rede devem ser adequadamente protegidas e criptografadas para corresponder à sua política de segurança. Você pode proteger toda a comunicação entre computadores Microsoft Windows usando IPSec; consulte a documentação do seu sistema operacional para obter detalhes sobre como fazer isso. Além disso, a comunicação entre dispositivos de usuário e desktops é protegida através do Citrix SecureICA, que é configurado por padrão para criptografia de 128 bits. Você pode configurar o SecureICA ao criar ou atualizar um Delivery Group.

> **Nota:**
>
> O Citrix SecureICA faz parte do protocolo ICA/HDX, mas não é um protocolo de segurança de rede compatível com padrões como o Transport Layer Security (TLS). Você também pode proteger as comunicações de rede entre dispositivos de usuário e desktops usando TLS. Para configurar o TLS, consulte Transport Layer Security (TLS).

> Aplique as melhores práticas do Windows para gerenciamento de contas. Não crie uma conta em um modelo ou imagem antes que ela seja duplicada pelo Machine Creation Services ou Provisioning Services. Não agende tarefas usando contas de domínio privilegiadas armazenadas. Não crie manualmente contas de máquina compartilhadas do Active Directory. Essas práticas ajudarão a evitar que um ataque de máquina obtenha senhas de contas persistentes locais e as use para fazer logon em imagens compartilhadas do MCS/PVS pertencentes a outros.

### Firewalls

Proteja todas as máquinas em seu ambiente com firewalls de perímetro, incluindo nas fronteiras de enclave, conforme apropriado.

Todas as máquinas em seu ambiente devem ser protegidas por um firewall pessoal. Ao instalar componentes principais e VDAs, você pode optar por ter as portas necessárias para a comunicação de componentes e recursos abertas automaticamente se o Serviço de Firewall do Windows for detectado (mesmo que o firewall não esteja ativado). Você também pode optar por configurar manualmente essas portas de firewall. Se você usar um firewall diferente, deverá configurá-lo manualmente.

Se você estiver migrando um ambiente convencional para esta versão, pode ser necessário reposicionar um firewall de perímetro existente ou adicionar novos firewalls de perímetro. Por exemplo, suponha que haja um firewall de perímetro entre um cliente convencional e um servidor de banco de dados no data center. Quando esta versão é usada, esse firewall de perímetro deve ser posicionado de forma que o desktop virtual e o dispositivo do usuário estejam de um lado, e os servidores de banco de dados e os Delivery Controllers no data center estejam do outro lado. Portanto, considere criar um enclave dentro do seu data center para conter os servidores de banco de dados e os Controllers. Considere também ter proteção entre o dispositivo do usuário e o desktop virtual.

> **Nota:**
>
> As portas TCP 1494 e 2598 são usadas para ICA e CGP e, portanto, provavelmente estarão abertas em firewalls para que usuários fora do data center possam acessá-las. A Citrix recomenda que você não use essas portas para mais nada, para evitar a possibilidade de deixar inadvertidamente interfaces administrativas abertas a ataques. As portas 1494 e 2598 são oficialmente registradas na Internet Assigned Number Authority (http://www.iana.org/).

### Segurança de aplicativos

Para evitar que usuários não administradores realizem ações maliciosas, recomendamos que você configure regras do Windows AppLocker para instaladores, aplicativos, executáveis e scripts no host VDA e no cliente Windows local.

## Gerenciar privilégios de usuário

Conceda aos usuários apenas os recursos de que eles precisam. Os privilégios do Microsoft Windows continuam sendo aplicados aos desktops da maneira usual: configure os privilégios por meio da Atribuição de Direitos de Usuário e as associações de grupo por meio da Política de Grupo. Uma vantagem desta versão é que é possível conceder a um usuário direitos administrativos a um desktop sem também conceder controle físico sobre o computador no qual o desktop está armazenado.

Observe o seguinte ao planejar os privilégios de desktop:

- Por padrão, quando usuários não privilegiados se conectam a um desktop, eles veem o fuso horário do sistema que executa o desktop em vez do fuso horário de seu próprio dispositivo de usuário. Para obter informações sobre como permitir que os usuários vejam a hora local ao usar desktops, consulte o artigo Gerenciar Grupos de Entrega.

- Um usuário que é administrador em um desktop tem controle total sobre esse desktop. Se um desktop for um desktop agrupado em vez de um desktop dedicado, o usuário deve ser confiável em relação a todos os outros usuários desse desktop, incluindo futuros usuários. Todos os usuários do desktop precisam estar cientes do risco potencial permanente à segurança de seus dados que essa situação representa. Essa consideração não se aplica a desktops dedicados, que têm apenas um único usuário; esse usuário não deve ser um administrador em nenhum outro desktop.
- Um usuário que é administrador em um desktop geralmente pode instalar software nesse desktop, incluindo software potencialmente malicioso. O usuário também pode potencialmente monitorar ou controlar o tráfego em qualquer rede conectada ao desktop.

## Gerenciar direitos de logon

Os direitos de logon são necessários para contas de usuário e contas de computador. Assim como os privilégios do Microsoft Windows, os direitos de logon continuam sendo aplicados aos desktops da maneira usual: configure os direitos de logon por meio da Atribuição de Direitos de Usuário e as associações de grupo por meio da Política de Grupo.

Os direitos de logon do Windows são: fazer logon localmente, fazer logon por meio dos Serviços de Área de Trabalho Remota, fazer logon pela rede (acessar este computador da rede), fazer logon como um trabalho em lote e fazer logon como um serviço.

Para contas de computador, conceda aos computadores apenas os direitos de logon de que eles precisam. O direito de logon "Acessar este computador da rede" é necessário:

- Em VDAs, para as contas de computador dos Delivery Controllers
- Em Delivery Controllers, para as contas de computador dos VDAs. Consulte Descoberta de Controller baseada em OU do Active Directory.
- Nos servidores StoreFront™, para as contas de computador de outros servidores no mesmo grupo de servidores StoreFront

Para contas de usuário, conceda aos usuários apenas os direitos de logon de que eles precisam.

De acordo com a Microsoft, por padrão, o grupo Usuários da Área de Trabalho Remota recebe o direito de logon "Permitir logon por meio dos Serviços de Área de Trabalho Remota" (exceto em controladores de domínio).

A política de segurança da sua organização pode declarar explicitamente que este grupo deve ser removido desse direito de logon. Considere a seguinte abordagem:

- O Virtual Delivery Agent (VDA) para SO multi-sessão usa os Serviços de Área de Trabalho Remota da Microsoft. Você pode configurar o grupo Usuários da Área de Trabalho Remota como um grupo restrito e controlar a associação do grupo por meio de políticas de grupo do Active Directory. Consulte a documentação da Microsoft para obter mais informações.
- Para outros componentes do Citrix Virtual Apps and Desktops™, incluindo o VDA para SO de sessão única, o grupo Usuários da Área de Trabalho Remota não é necessário. Portanto, para esses componentes, o grupo Usuários da Área de Trabalho Remota não requer o direito de logon "Permitir logon por meio dos Serviços de Área de Trabalho Remota"; você pode removê-lo. Além disso:
  - Se você administra esses computadores por meio dos Serviços de Área de Trabalho Remota, certifique-se de que todos esses administradores já sejam membros do grupo Administradores.
  - Se você não administra esses computadores por meio dos Serviços de Área de Trabalho Remota, considere desabilitar os próprios Serviços de Área de Trabalho Remota nesses computadores.

Embora seja possível adicionar usuários e grupos ao direito de logon "Negar logon por meio dos Serviços de Área de Trabalho Remota", o uso de direitos de logon de negação geralmente não é recomendado. Consulte a documentação da Microsoft para obter mais informações.

## Configurar direitos de usuário

A instalação do Delivery Controller™ cria os seguintes serviços do Windows:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Gerencia contas de computador do Microsoft Active Directory para VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Coleta informações de uso da configuração do site para uso pela Citrix, se essa coleta tiver sido aprovada pelo administrador do site. Em seguida, envia essas informações para a Citrix, para ajudar a melhorar o produto.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Suporta o gerenciamento e o provisionamento de AppDisks, integração do AppDNA e gerenciamento do App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Seleciona os desktops virtuais ou aplicativos que estão disponíveis para os usuários.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Registra todas as alterações de configuração e outras alterações de estado feitas pelos administradores no site.

- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Repositório em todo o site para configuração compartilhada.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Gerencia as permissões concedidas aos administradores.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Gerencia autotestes dos outros serviços do Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService): Armazena informações sobre as infraestruturas de hipervisor usadas em uma implantação do Citrix Virtual Apps ou Citrix Virtual Desktops e também oferece funcionalidade usada pelo console para enumerar recursos em um pool de hipervisores.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): Orquestra a criação de VMs de desktop.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Coleta métricas para Citrix Virtual Apps ou Citrix Virtual Desktops, armazena informações históricas e fornece uma interface de consulta para ferramentas de solução de problemas e relatórios.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): Suporta o gerenciamento do StoreFront. (Não faz parte do próprio componente StoreFront.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Suporta operações de gerenciamento privilegiado do StoreFront. (Não faz parte do próprio componente StoreFront.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): Propaga dados de configuração do banco de dados principal do site para o Cache de Host Local.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): Seleciona os desktops virtuais ou aplicativos que estão disponíveis para os usuários, quando o banco de dados principal do site está indisponível.

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Eles também são criados quando instalados com outros componentes Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Suporta a coleta de informações de diagnóstico para uso pelo Suporte Citrix.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Coleta informações de diagnóstico para análise pela Citrix, de modo que os resultados da análise e as recomendações possam ser visualizados pelos administradores para ajudar a diagnosticar problemas com o site.

A instalação do Delivery Controller também cria o seguinte serviço do Windows. Este não está sendo usado atualmente. Se tiver sido ativado, desative-o.

- Provedor de Broker Remoto Citrix (NT SERVICE\XaXdCloudProxy)

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Estes não são usados atualmente, mas devem ser habilitados. Não os desabilite.

- Serviço de Orquestração Citrix (NT SERVICE\CitrixOrchestration)
- Serviço de Confiança Citrix (NT SERVICE\CitrixTrust)

Com exceção do Serviço de Administração Privilegiada do Citrix Storefront, esses serviços recebem o direito de logon Fazer logon como um serviço e os privilégios Ajustar cotas de memória para um processo, Gerar auditorias de segurança e Substituir um token de nível de processo. Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Delivery Controller e são desabilitados automaticamente.

## Configurar configurações de serviço

Com exceção do serviço de Administração Privilegiada do Citrix Storefront e do Serviço de Telemetria Citrix, os serviços do Windows do Delivery Controller listados acima na seção Configurar direitos de usuário são configurados para fazer logon como a identidade NETWORK SERVICE. Não altere essas configurações de serviço.

O Serviço de Sincronização de Configuração Citrix precisa que a conta NETWORK SERVICE pertença ao grupo de Administradores Locais no Delivery Controller. Isso permite que o Cache de Host Local funcione corretamente.

O serviço de Administração Privilegiada do Citrix Storefront é configurado para fazer logon como Sistema Local (NT AUTHORITY\SYSTEM). Isso é necessário para operações do StoreFront do Delivery Controller que normalmente não estão disponíveis para serviços (incluindo a criação de sites do Microsoft IIS). Não altere suas configurações de serviço.

O Serviço de Telemetria Citrix é configurado para fazer logon como sua própria identidade específica de serviço.

Você pode desabilitar o Serviço de Telemetria Citrix. Além deste serviço e dos serviços que já estão desabilitados, não desabilite nenhum outro desses serviços do Windows do Delivery Controller.

## Configurar configurações de registro

Não é mais necessário habilitar a criação de nomes de arquivo e pastas 8.3 no sistema de arquivos VDA. A chave de registro **NtfsDisable8dot3NameCreation** pode ser configurada para desabilitar a criação de nomes de arquivo e pastas 8.3. Você também pode configurar isso usando o comando **fsutil.exe behavior set disable8dot3**.

## Implicações de segurança do cenário de implantação

Seu ambiente de usuário pode conter dispositivos de usuário que não são gerenciados pela sua organização e estão completamente sob o controle do usuário, ou dispositivos de usuário que são gerenciados e administrados pela sua organização. As considerações de segurança para esses dois ambientes são geralmente diferentes.

### Dispositivos de usuário gerenciados

Dispositivos de usuário gerenciados estão sob controle administrativo; eles estão sob seu próprio controle ou sob o controle de outra organização em que você confia. Você pode configurar e fornecer dispositivos de usuário diretamente aos usuários; alternativamente, você pode fornecer terminais nos quais um único desktop é executado apenas no modo de tela cheia. Siga as melhores práticas gerais de segurança descritas acima para todos os dispositivos de usuário gerenciados. Esta versão tem a vantagem de que um software mínimo é necessário em um dispositivo de usuário.

Um dispositivo de usuário gerenciado pode ser configurado para ser usado apenas no modo de tela cheia ou no modo de janela:

- Modo somente tela cheia: Os usuários fazem logon com a tela usual de Log On To Windows. As mesmas credenciais de usuário são então usadas para fazer logon automaticamente nesta versão.
- Os usuários veem seu desktop em uma janela: Os usuários primeiro fazem logon no dispositivo de usuário e, em seguida, fazem logon nesta versão por meio de um site fornecido com a versão.

### Dispositivos de usuário não gerenciados

Não se pode presumir que dispositivos de usuário que não são gerenciados e administrados por uma organização confiável estejam sob controle administrativo. Por exemplo, você pode permitir que os usuários obtenham e configurem seus próprios dispositivos, mas os usuários podem não seguir as melhores práticas gerais de segurança descritas acima. Esta versão tem a vantagem de que é possível entregar desktops com segurança a dispositivos de usuário não gerenciados.

Esses dispositivos ainda devem ter proteção antivírus básica que combaterá keyloggers e ataques de entrada semelhantes.

### Considerações sobre armazenamento de dados

Ao usar esta versão, você pode impedir que os usuários armazenem dados em dispositivos de usuário que estão sob seu controle físico. No entanto, você ainda deve considerar as implicações de os usuários armazenarem dados em desktops. Não é uma boa prática para os usuários armazenarem dados em desktops; os dados devem ser mantidos em servidores de arquivos, servidores de banco de dados ou outros repositórios onde possam ser protegidos adequadamente.

Seu ambiente de desktop pode consistir em vários tipos de desktops, como desktops agrupados (pooled) e dedicados. Os usuários nunca devem armazenar dados em desktops que são compartilhados entre usuários, como desktops agrupados. Se os usuários armazenarem dados em desktops dedicados, esses dados devem ser removidos se o desktop for posteriormente disponibilizado para outros usuários.

### Ambientes de versão mista

Ambientes de versão mista são inevitáveis durante algumas atualizações. Siga as melhores práticas e minimize o tempo em que os componentes Citrix de diferentes versões coexistem. Em ambientes de versão mista, a política de segurança, por exemplo, pode não ser aplicada uniformemente.

> **Nota:**
>
> Isso é típico de outros produtos de software; o uso de uma versão anterior do Active Directory apenas aplica parcialmente a Política de Grupo com versões posteriores do Windows.

> O cenário a seguir descreve um problema de segurança que pode ocorrer em um ambiente Citrix de versão mista específico. Quando o Citrix Receiver 1.7 é usado para conectar-se a um desktop virtual executando o VDA no XenApp and XenDesktop 7.6 Feature Pack 2, a configuração de política **Allow file transfer between desktop and client** está habilitada no Site, mas não pode ser desabilitada por um Delivery Controller executando o XenApp and XenDesktop 7.1. Ele não reconhece a configuração de política, que foi lançada em uma versão posterior do produto. Essa configuração de política permite que os usuários carreguem e baixem arquivos para seu desktop virtual, o que é o problema de segurança.

> Para contornar isso, atualize o Delivery Controller (ou uma instância autônoma do Studio) para a versão 7.6 Feature Pack 2 e, em seguida, use a Política de Grupo para desabilitar a configuração de política. Alternativamente, use a política local em todos os desktops virtuais afetados.

## Considerações de segurança do Acesso Remoto para PC

O Acesso Remoto a PC implementa os seguintes recursos de segurança:

- O uso de cartão inteligente é suportado.
- Quando uma sessão remota se conecta, o monitor do PC do escritório aparece em branco.
- O Acesso Remoto a PC redireciona todas as entradas de teclado e mouse para a sessão remota, exceto CTRL+ALT+DEL e cartões inteligentes habilitados para USB e dispositivos biométricos.
- O SmoothRoaming é suportado apenas para um único usuário.
- Quando um usuário tem uma sessão remota conectada a um PC de escritório, somente esse usuário pode retomar o acesso local ao PC de escritório. Para retomar o acesso local, o usuário pressiona Ctrl-Alt-Del no PC local e, em seguida, faz login com as mesmas credenciais usadas pela sessão remota. O usuário também pode retomar o acesso local inserindo um cartão inteligente ou utilizando biometria, se o seu sistema tiver a integração apropriada de Provedor de Credenciais de terceiros. Esse comportamento padrão pode ser substituído ativando a Troca Rápida de Usuário por meio de Objetos de Política de Grupo (GPOs) ou editando o registro.

**Nota:**

> A Citrix recomenda que você não atribua privilégios de administrador de VDA a usuários de sessão gerais.

### Atribuições automáticas

Por padrão, o Acesso Remoto a PC suporta a atribuição automática de vários usuários a um VDA. No XenDesktop 5.6 Feature Pack 1, os administradores podiam substituir esse comportamento usando o script PowerShell RemotePCAccess.ps1. Esta versão usa uma entrada de registro para permitir ou proibir várias atribuições automáticas de PC remoto; essa configuração se aplica a todo o Site.

> **Cuidado:**

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

> Para restringir atribuições automáticas a um único usuário:

Em cada Controller no Site, defina a seguinte entrada de registro:

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

Se houver atribuições de usuário existentes, remova-as usando comandos SDK para que o VDA seja subsequentemente elegível para uma única atribuição automática.

- Remova todos os usuários atribuídos do VDA: `$machine.AssociatedUserNames | % { Remove-BrokerUser-Name $_ -Machine $machine`
- Remova o VDA do Grupo de Entrega: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Reinicie o PC físico do escritório.

## Confiança XML

A configuração de confiança XML se aplica a implantações que usam:

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

Habilitar a configuração de confiança XML permite que os usuários autenticar com sucesso e, em seguida, iniciem aplicativos. O Delivery Controller confia nas credenciais enviadas do StoreFront. Habilite esta configuração apenas quando tiver comunicações seguras entre seus Delivery Controllers e StoreFront (usando firewalls, IPsec ou outras recomendações de segurança).

Esta configuração está desabilitada por padrão.

Use o SDK do PowerShell do Citrix Virtual Apps and Desktops para verificar, habilitar ou desabilitar a configuração de confiança XML.

- Para verificar o valor atual da configuração de confiança XML, execute `Get-BrokerSite` e inspecione o valor de `TrustRequestsSentToTheXMLServicePort`.
- Para habilitar a confiança XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`.
- Para desabilitar a confiança XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`.

# Gerenciar certificados

O TLS usa certificados para estabelecer confiança entre duas partes. Você deve instalar um certificado adequado em cada servidor que fornece um serviço e garantir que as máquinas que se conectam a esse servidor confiem nesse certificado. Existem as seguintes opções para assinar certificados:

- Certificados autoassinados. Não são recomendados. São difíceis de gerenciar, pois você deve copiar manualmente este certificado para qualquer outra máquina que precise confiar nele.
- Autoridade de certificação corporativa. Se você já possui uma PKI implementada, esta é normalmente a opção mais simples para assinar certificados para uso entre dispositivos internos.
- Autoridade de certificação pública. Isso exige que você comprove a propriedade do domínio à autoridade de certificação. Tem a vantagem de que os dispositivos cliente não gerenciados são normalmente pré-configurados para confiar em certificados de grandes autoridades de certificação públicas.

## Criar um novo certificado

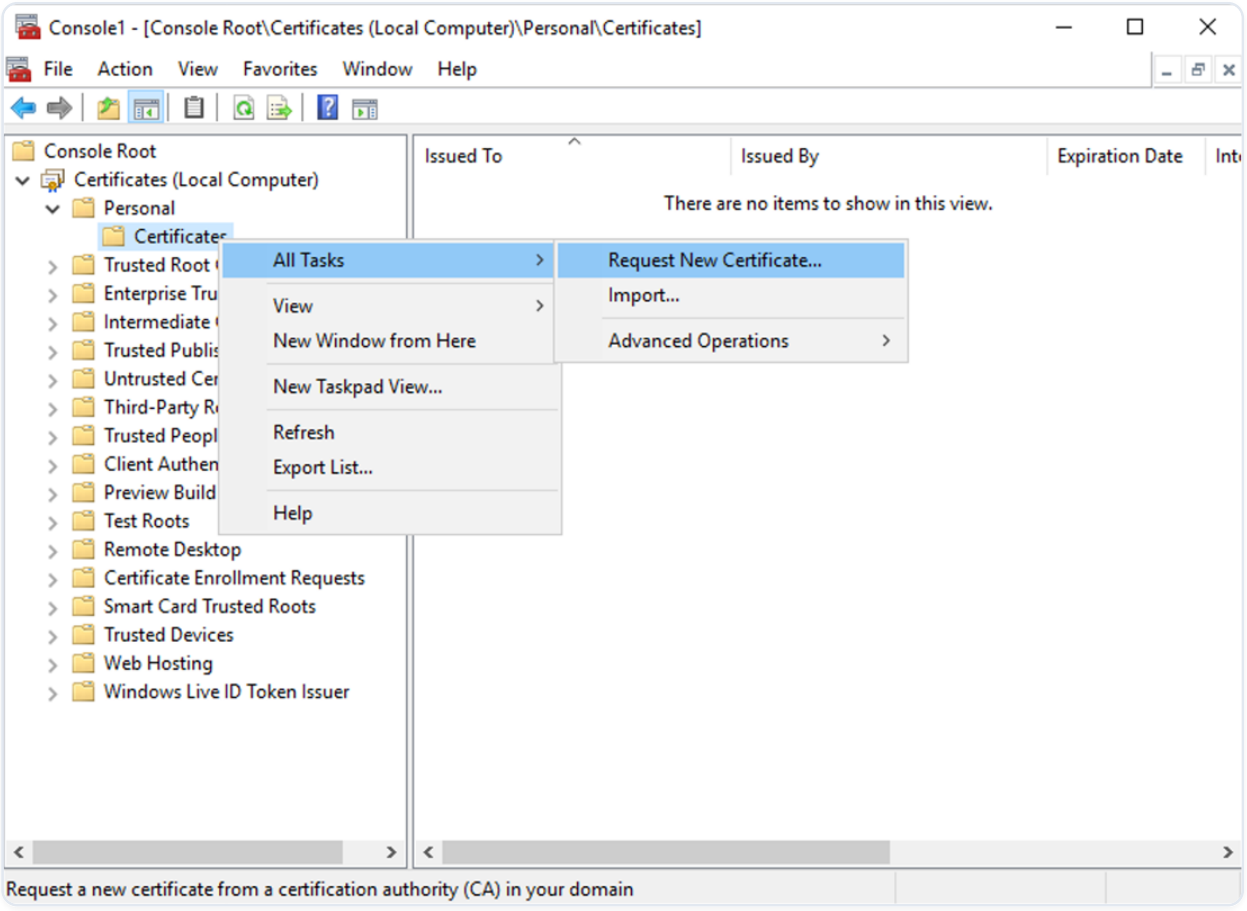
Siga as políticas e procedimentos da sua organização para criar certificados.

### Criar certificado usando a Autoridade de Certificação Microsoft

Se a Autoridade de Certificação Microsoft estiver integrada a um domínio do Active Directory ou à floresta confiável à qual os Delivery Controllers estão conectados, você poderá adquirir um certificado do assistente de Registro de Certificado do snap-in Certificados do MMC. A Autoridade de Certificação Microsoft precisa ter um modelo de certificado publicado adequado para uso por servidores web.

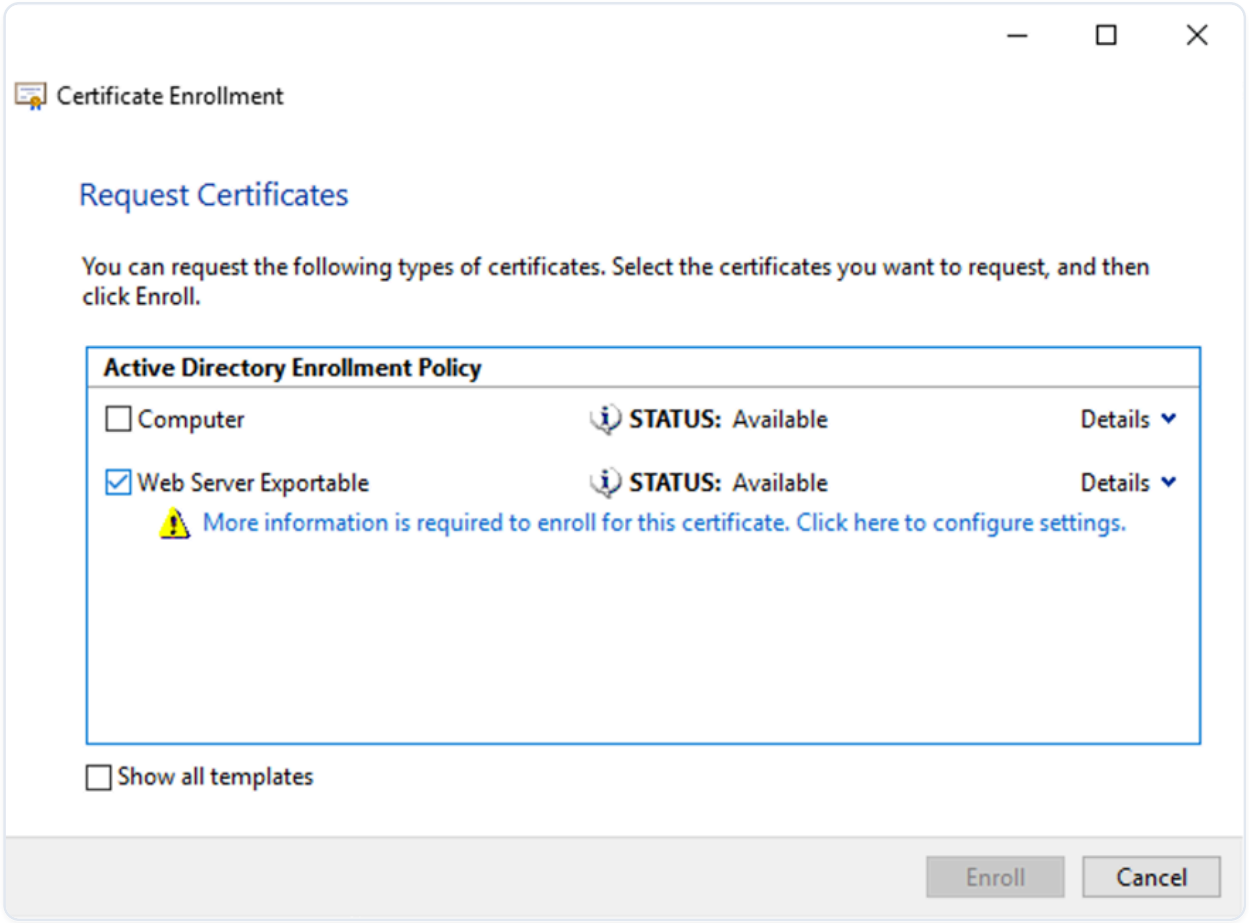
O certificado raiz é implantado automaticamente em outras máquinas no domínio usando a política de grupo. Portanto, todas as outras máquinas no domínio confiam em certificados criados usando a Autoridade de Certificação Microsoft. Se você tiver máquinas fora do domínio, precisará exportar o Certificado da Autoridade de Certificação Raiz e importá-lo para essas máquinas.

1. No servidor, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando do menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.




3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.

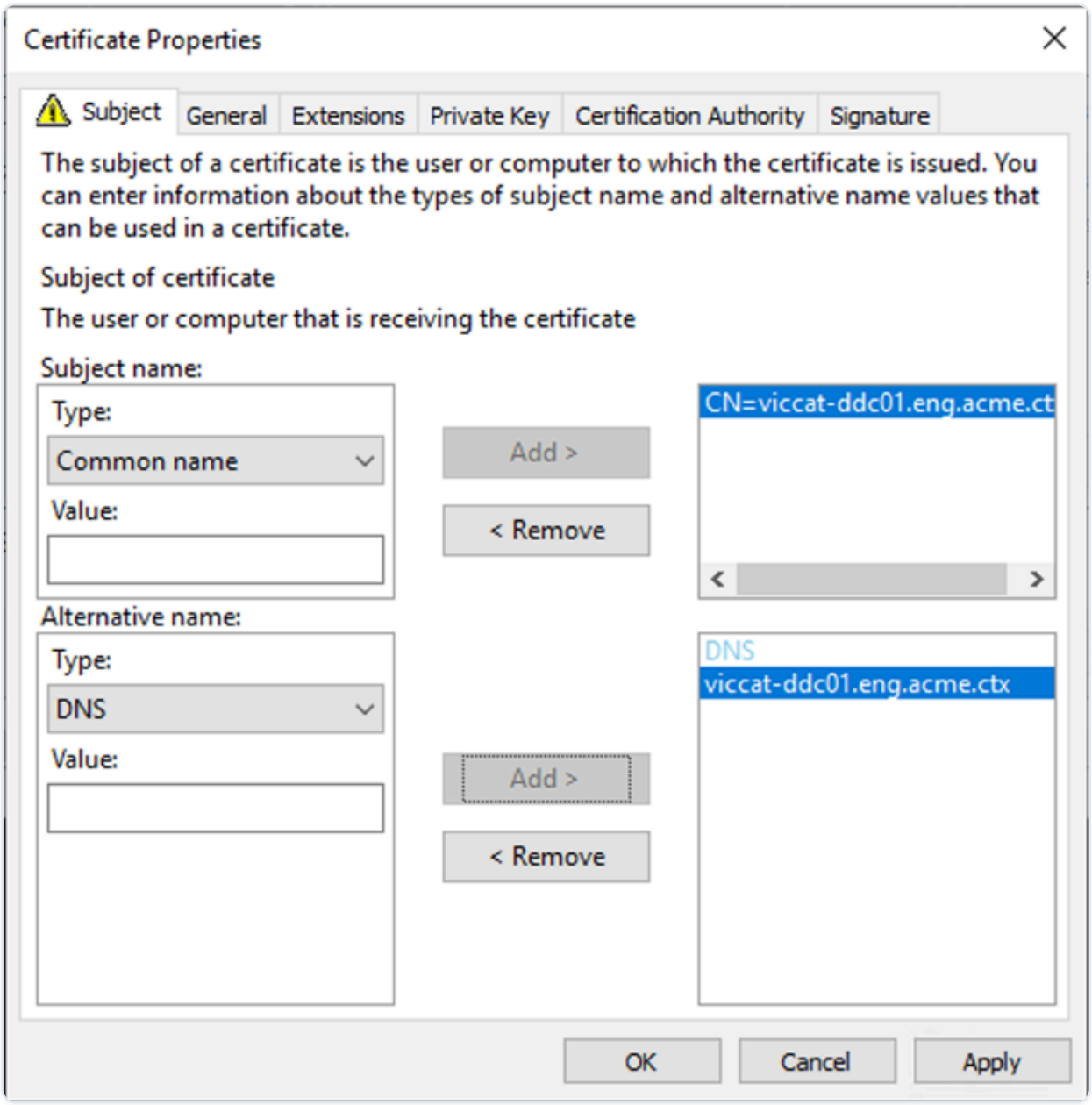
4. Selecione um modelo adequado, como **Servidor Web Exportável**. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você pode clicar em **Registrar** sem fornecer mais detalhes. Caso contrário, clique em **Mais informações são necessárias para registrar este certificado. Clique aqui para configurar as definições.**



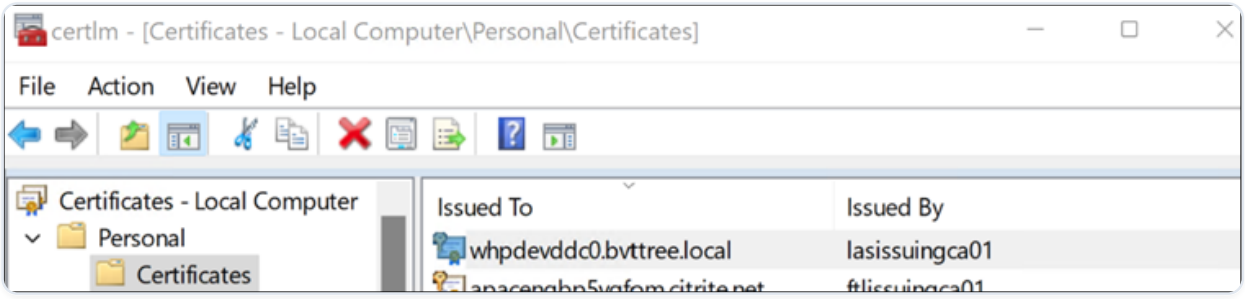

5. Para fornecer mais detalhes para o modelo de certificado, clique no botão de seta **Detalhes** e configure o seguinte:

   **Nome do assunto**: selecione Nome Comum e adicione o FQDN do servidor.

   **Nome alternativo**: selecione DNS e adicione o FQDN do servidor.




6. Pressione **OK**.
7. Pressione **Registrar** para criar o certificado. Ele é exibido na lista de certificados.



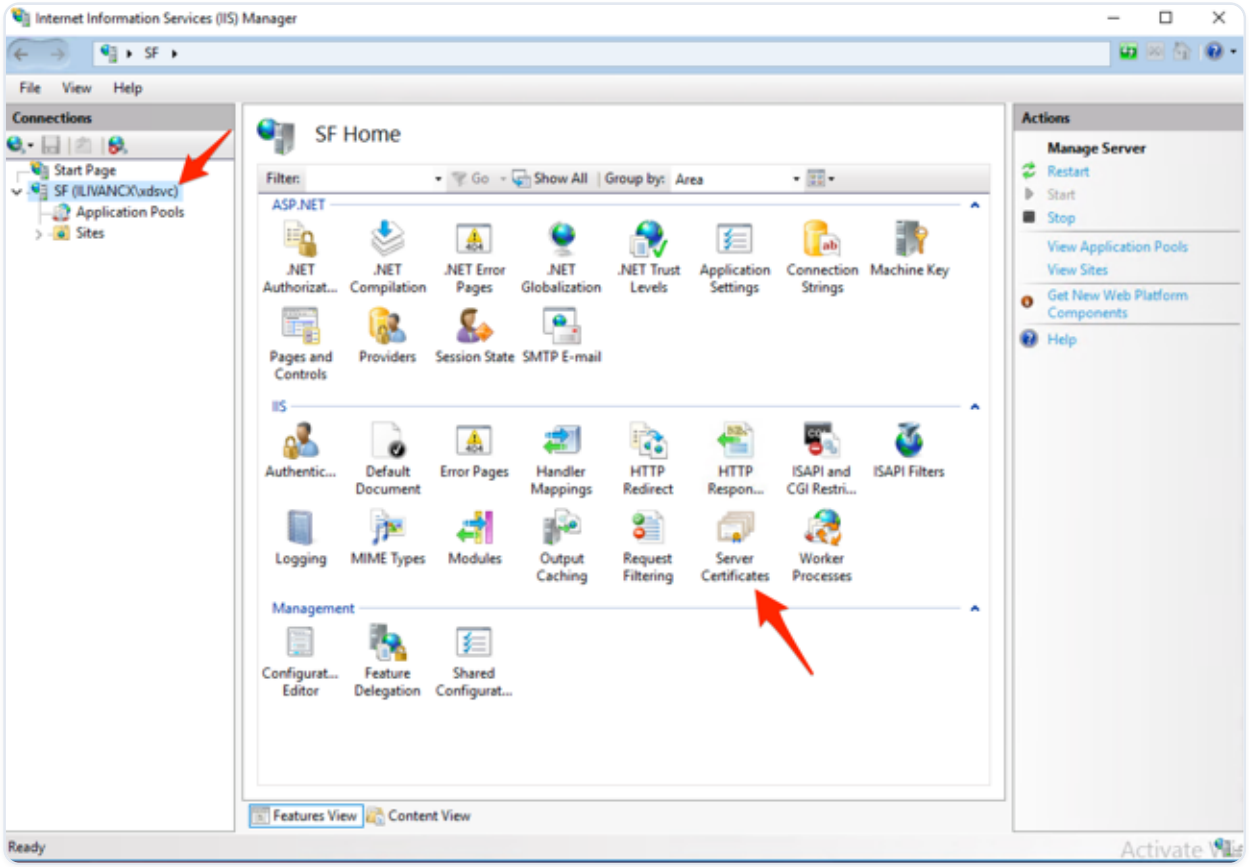

## Criar uma solicitação de certificado usando o IIS

Se o IIS estiver instalado no servidor então conclua as seguintes etapas:

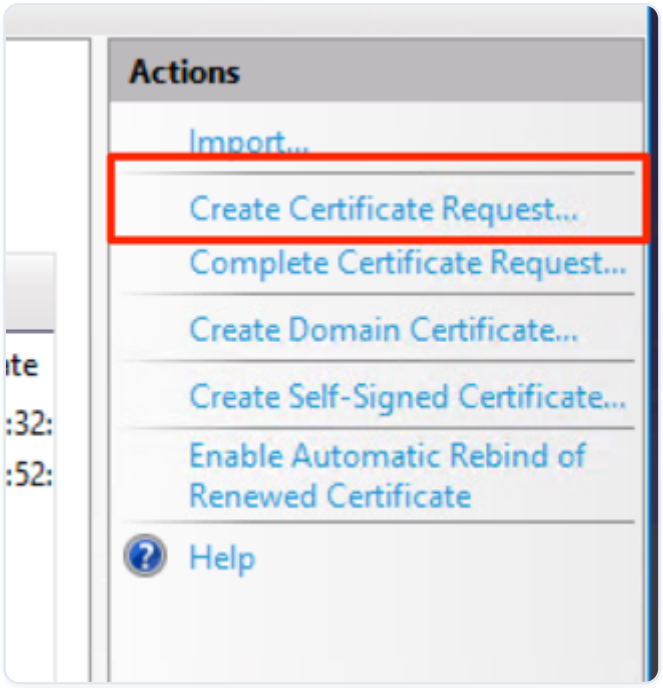
1. Abra o **Gerenciador do Internet Information Service (IIS)**

2. Selecione o nó do servidor na lista Conexões.

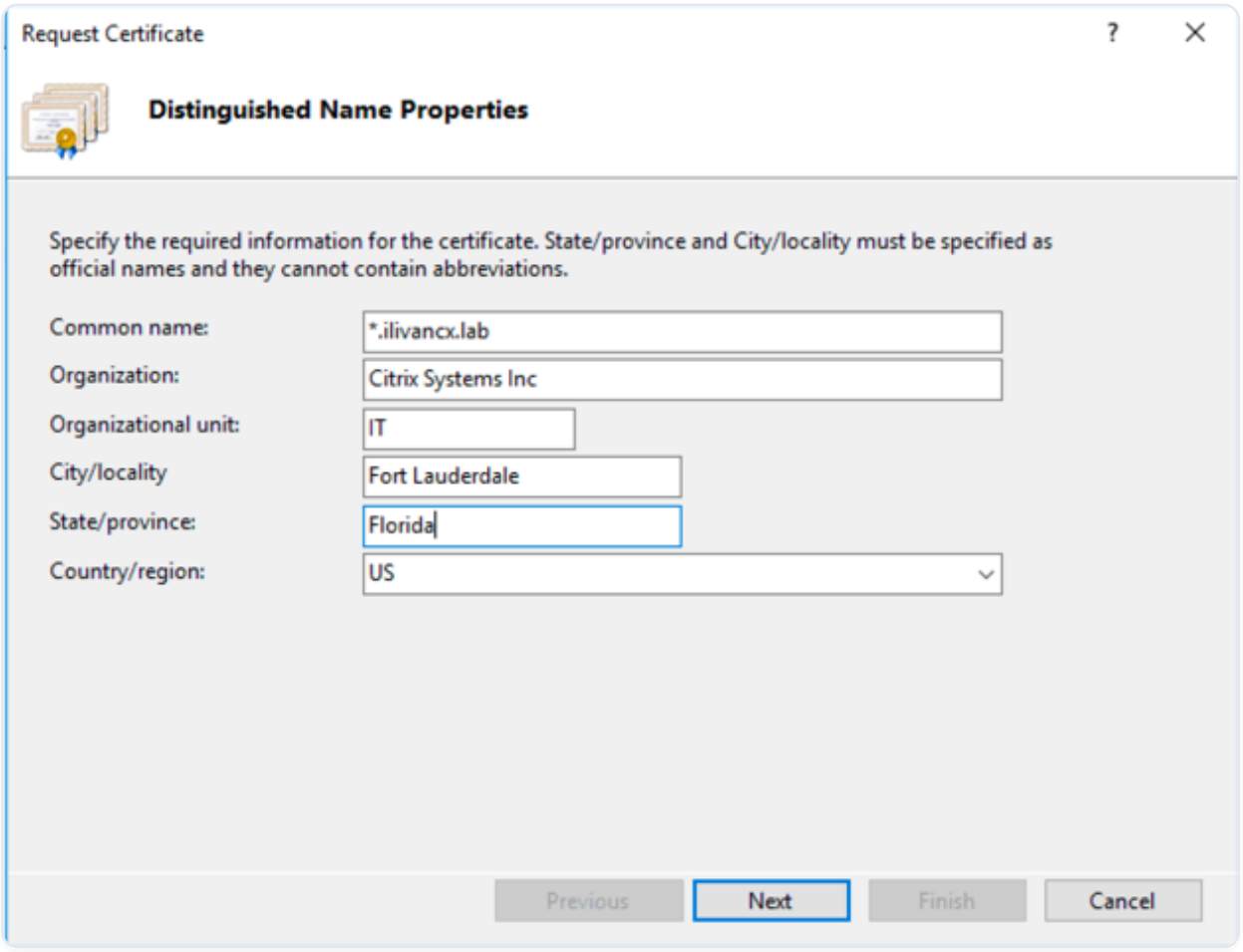
3. Abra **Certificados do Servidor**.



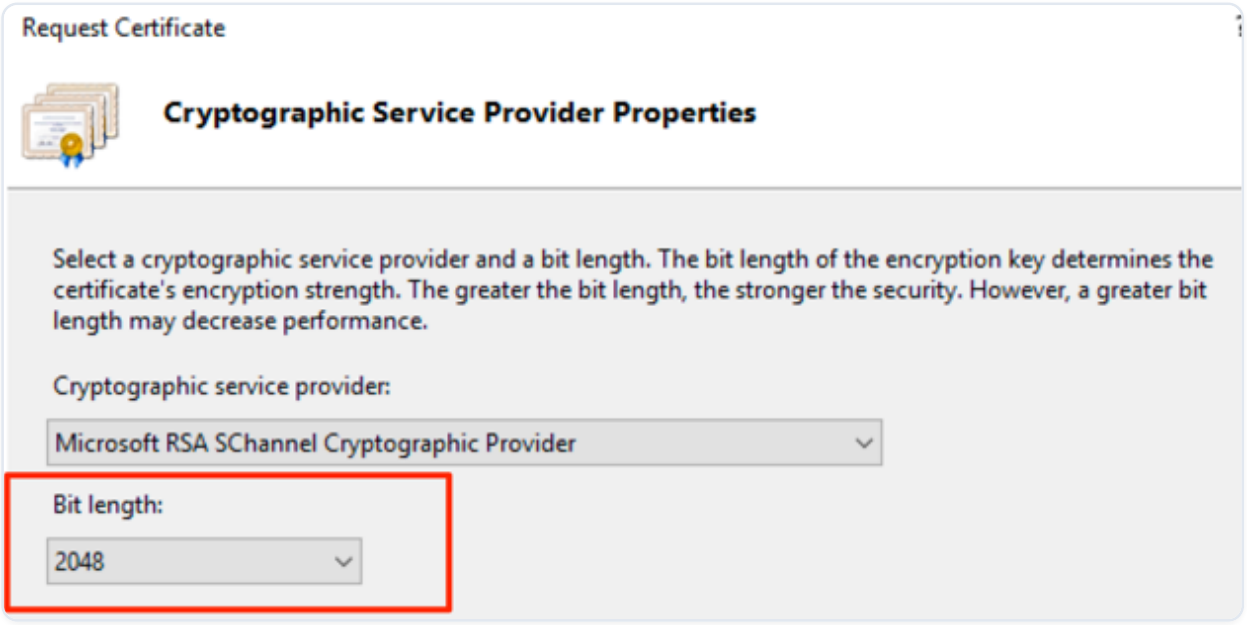

4. No painel **Ações**, selecione **Criar Solicitação de Certificado...**.



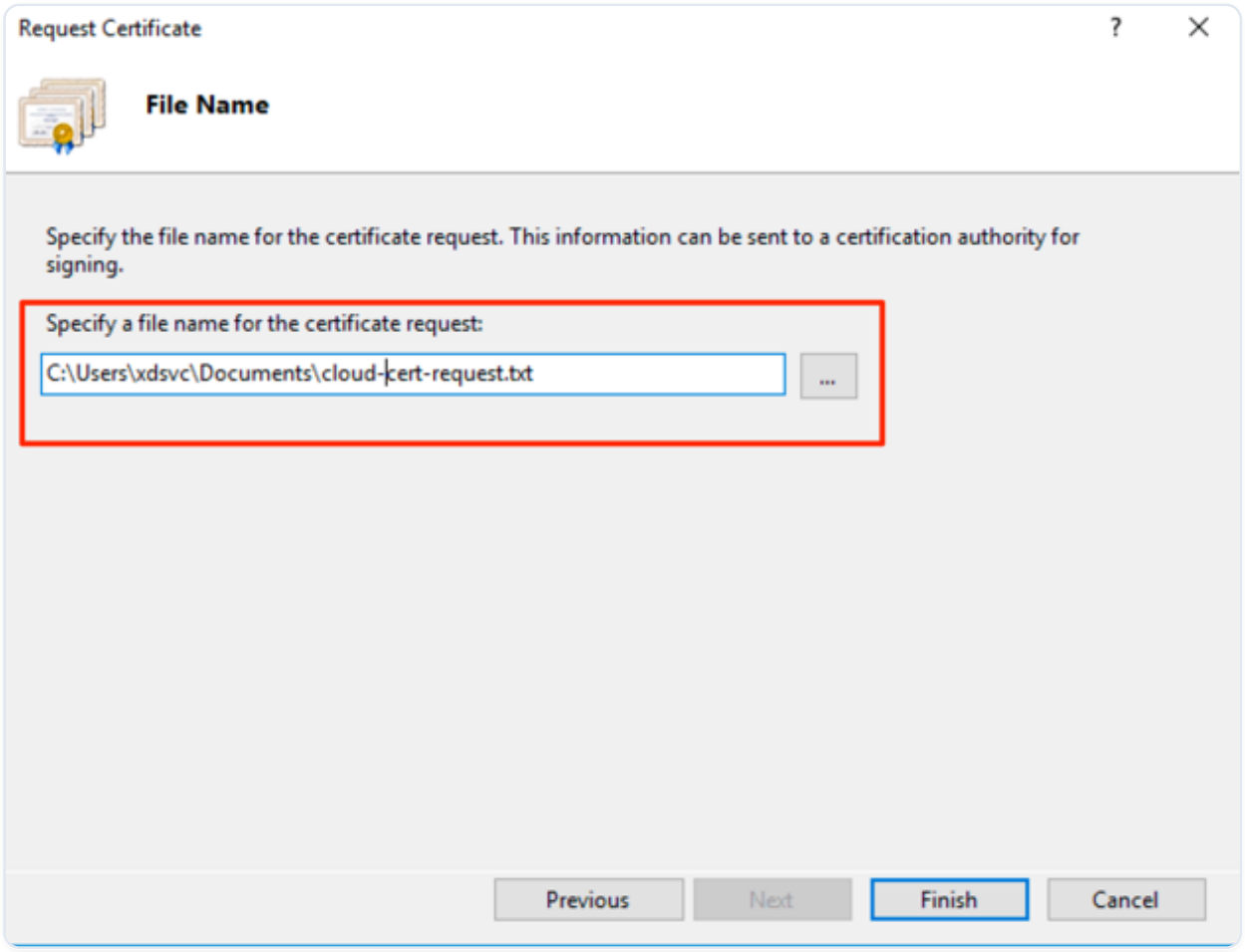
5. Insira as **Propriedades do nome distinto**.



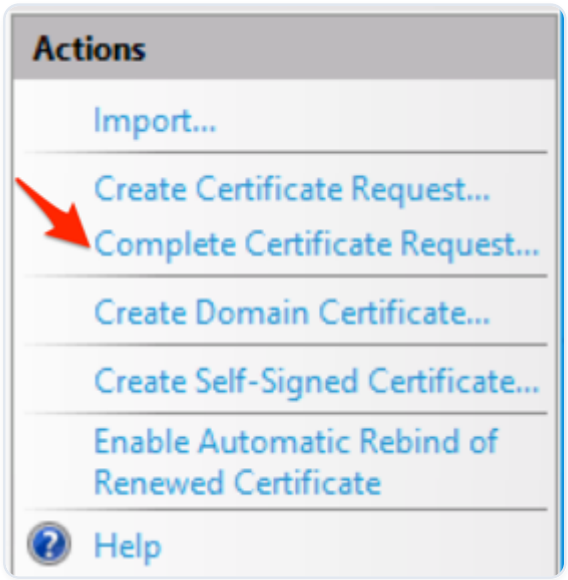

6. Na tela **Propriedades do Provedor de Serviço Criptográfico**, deixe o **Provedor de serviço criptográfico** como padrão. Selecione um tamanho de chave de **2048** ou superior.



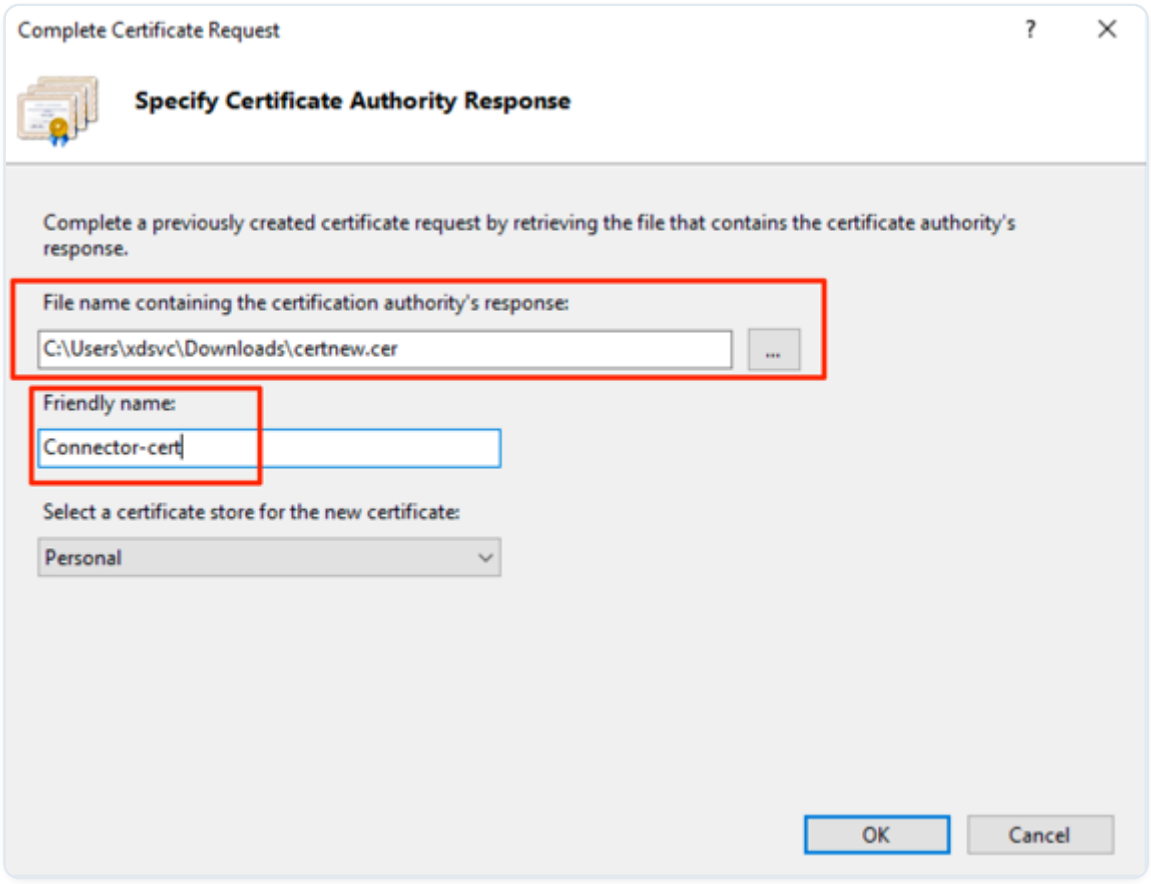
7. Escolha um nome de arquivo e pressione **Concluir**.




8. Carregue seu CSR para sua autoridade de certificação.
9. Depois de receber o certificado, no painel **Ações**, selecione **Concluir Solicitação de Certificado...**.



10. Selecione o certificado, forneça um **Nome amigável** e pressione **OK**.




Não há como definir o nome alternativo do assunto. Portanto, o certificado é limitado ao servidor especificado usando o nome comum.

### Criar uma solicitação de assinatura de certificado a partir do snap-in de certificados

Dentro do snap-in MMC de Certificados, você pode criar uma solicitação de assinatura de certificado. Isso gera um arquivo que você pode enviar a uma autoridade de certificação que fornecerá o certificado. Você deve então importar o certificado para combiná-lo com a chave privada local.

1. No servidor, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal** > **Certificados**
3. Selecione **Todas as Tarefas** > **Operações Avançadas** > **Criar Solicitação Personalizada**.
4. Em **Antes de Começar**, selecione **Avançar**.
5. Na tela **Selecionar Política de Registro de Certificado**, selecione uma política existente adequada ou **Continuar sem política de registro**.
6. Na tela **Solicitação personalizada**, se estiver usando uma política de registro, escolha um modelo apropriado, se disponível, como **Servidor Web Exportável**.

7. Na tela **Informações do Certificado**, expanda **Detalhes** e selecione **Propriedades**.
8. Na janela **Propriedades do Certificado**, na guia **Geral**, insira um nome amigável adequado.
9. Na guia **Assunto**:
    a. Em **Nome do assunto**, selecione **Nome comum** e insira o FQDN do servidor. Você pode inserir um curinga. Selecione **Adicionar**.
    b. Em **Nome do assunto**, adicione valores apropriados para Organização, Unidade Organizacional, Localidade, Estado, País.
    c. Em **Nome alternativo**, selecione **DNS**. Adicione o FQDN do servidor. Você pode adicionar vários FQDNs de servidor ou um FQDN curinga.
10. Na guia **Extensões**:
    - Em **Uso da chave**, adicione **Assinatura digital** e **Criptografia de chave**.
    - Em **Uso de chave estendido (políticas de aplicativo)**, adicione **Autenticação de servidor** e **Autenticação de cliente**.
11. Na guia **Chave Privada**.
    - Em **Selecionar Provedor de Serviços Criptográficos (CSP)**, escolha um provedor adequado.
    - Em **Opções de chave**, selecione um tamanho de chave adequado. Para provedores RSA, use no mínimo um tamanho de chave de 2048. Para maior segurança, você pode querer escolher 4096, mas isso terá um leve impacto no desempenho.
    - Em **Opções de chave**, selecione **Tornar chave privada exportável**.
12. Selecione **OK**.
13. Selecione **Avançar**.
14. Selecione **Procurar** e salve sua solicitação.
15. Selecione **Concluir**.
16. Carregue seu CSR para sua autoridade de certificação.
17. Uma vez que você tenha recebido o certificado, importe-o no mesmo servidor para que ele seja vinculado à chave privada.

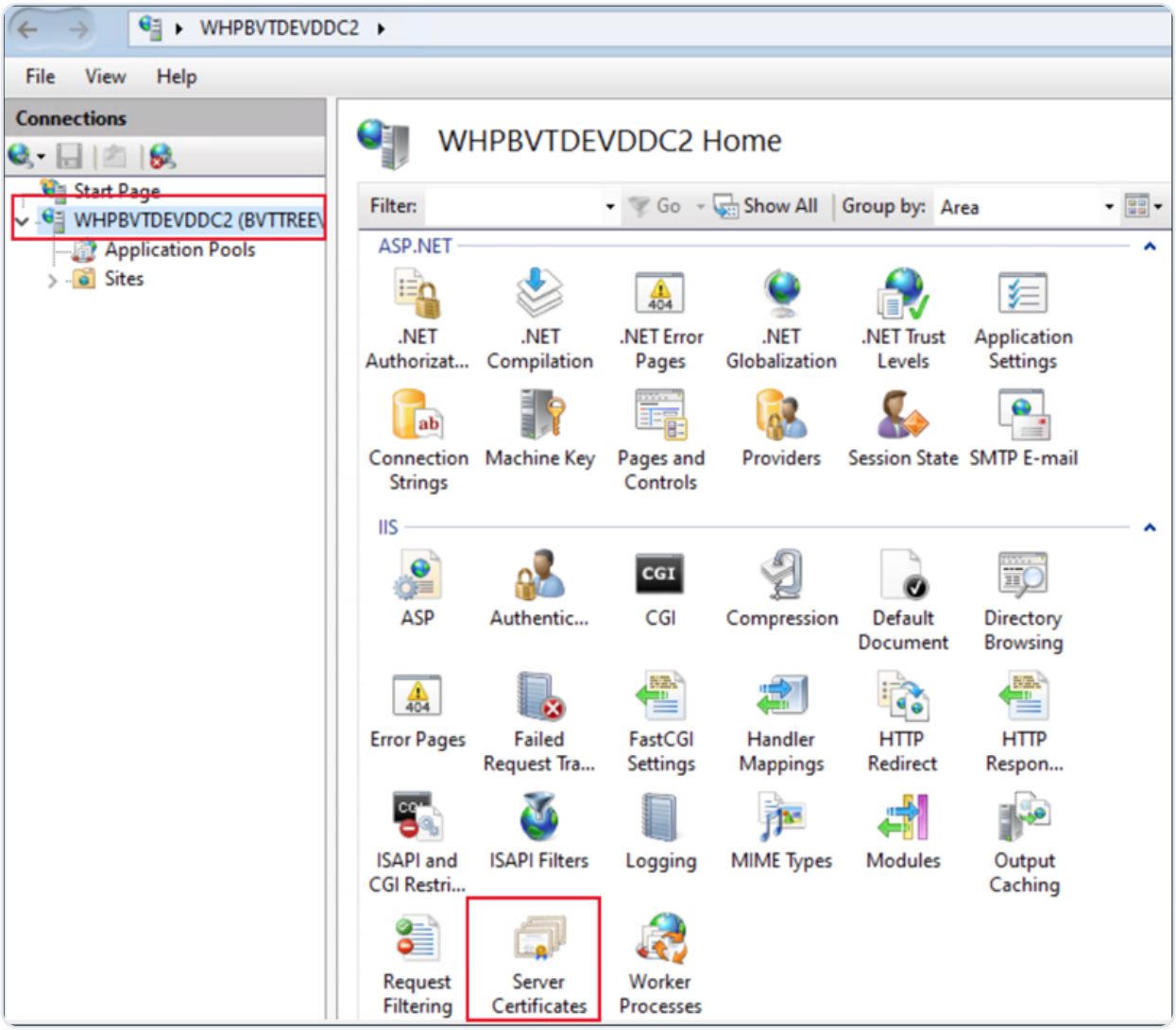
### Criar um novo certificado autoassinado

Um certificado autoassinado é criado durante a instalação de um controlador de entrega™ e do web studio. Você pode gerar um novo certificado autoassinado e usá-lo para substituir o existente.

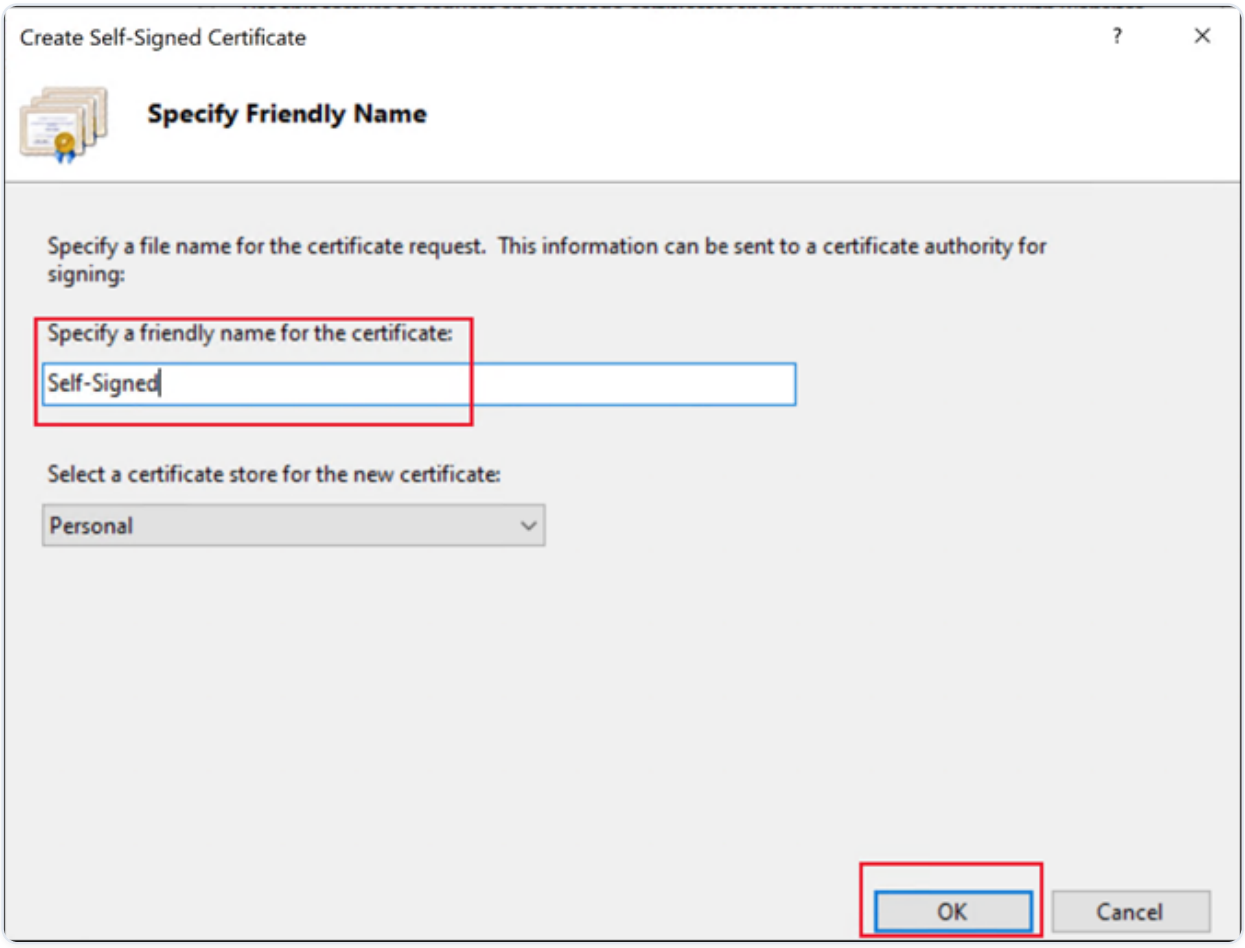
### Usando o Gerenciador do IIS

Se o IIS estiver instalado no servidor, você poderá executar as seguintes etapas:

1. Faça logon no servidor como administrador.
2. Abra o Gerenciador do IIS
3. Abra **Certificados de Servidor**
4. No painel **Ações**, selecione **Criar Certificado Autoassinado**.




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




### Usando o PowerShell

Você pode usar o PowerShell para criar um certificado autoassinado:

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"

$expireYears = 5



## Create new self-signed certificate under LocalMachine\My

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

```
# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)

$rootCertStore.Add($certificate)
```

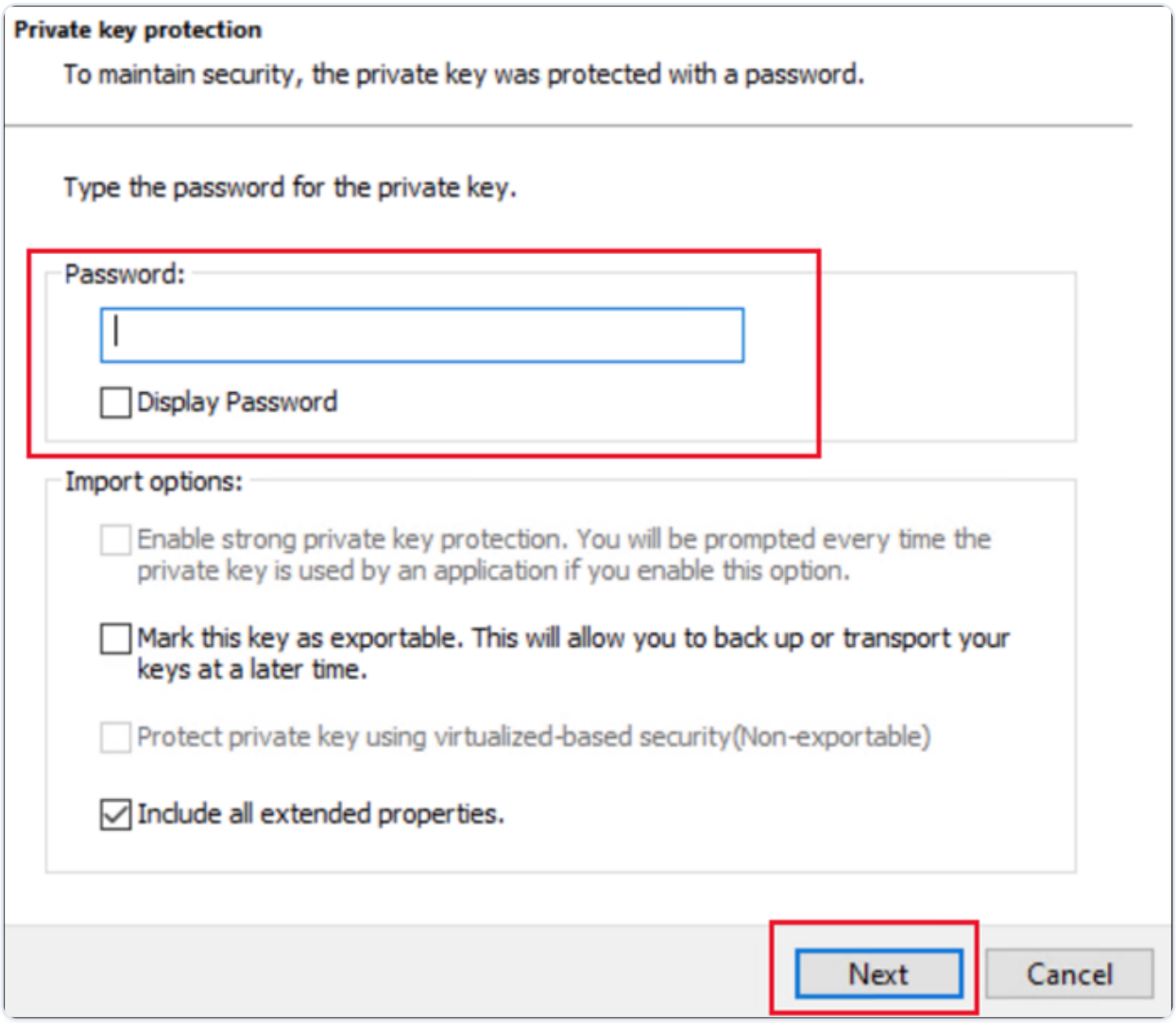
## Importar certificado existente

Você pode importar um certificado existente para o servidor usando qualquer um dos seguintes métodos.

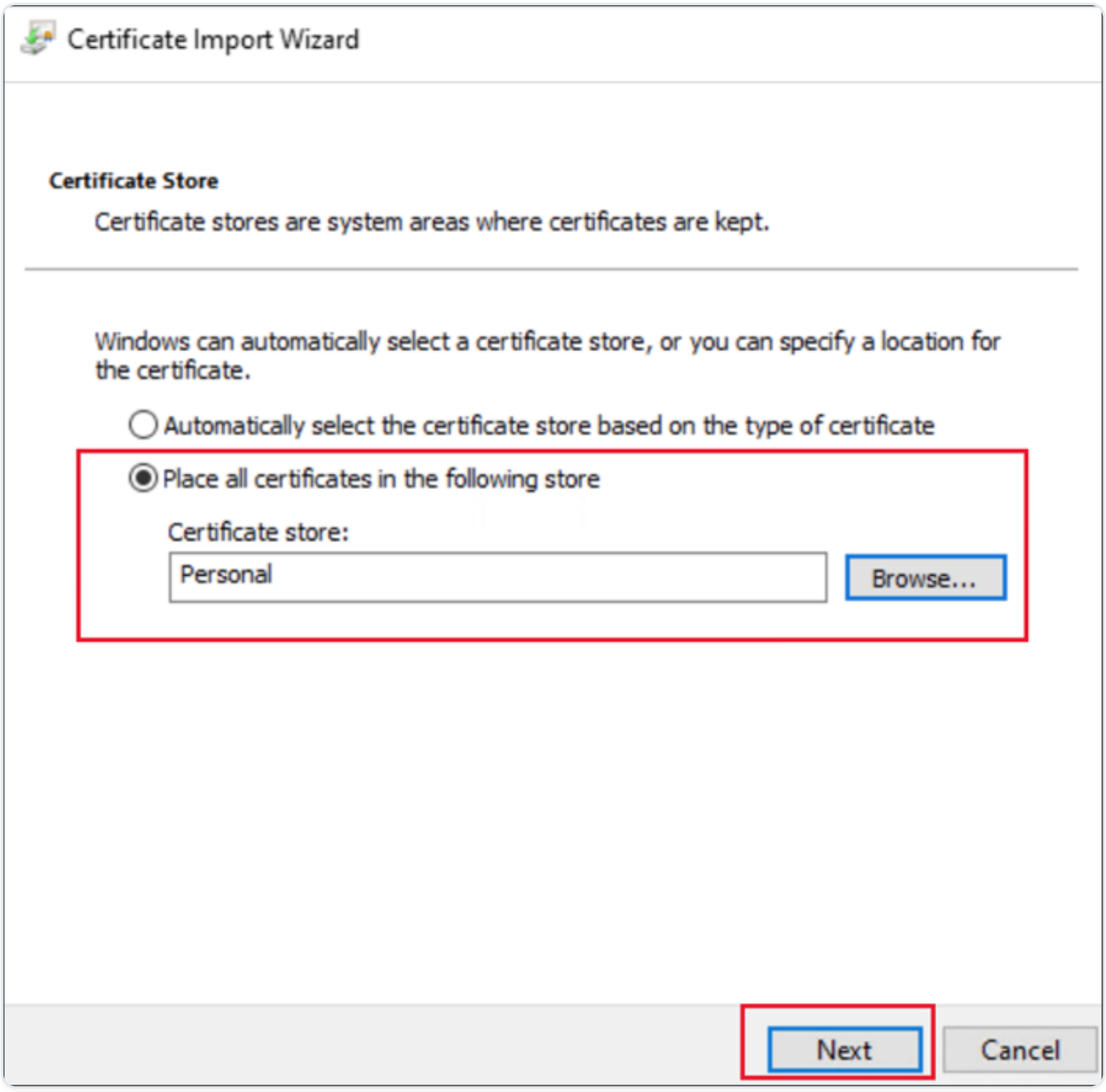
### Assistente de importação de certificado

1. Clique duas vezes no arquivo PFX ou clique com o botão direito do mouse no arquivo e selecione **Instalar PFX**. Isso abre o **Assistente de Importação de Certificado**.
2. Para **Local do Repositório**, selecione **Máquina Local**.

   Captura de tela do assistente de importação de certificado(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-import-wizard.png)
3. Insira a senha, se necessário.




4. Selecione o **Repositório de Certificados**. Para certificados de servidor, escolha **Pessoal**. Se for um certificado raiz ou autoassinado que você deseja confiar nesta máquina, escolha **Autoridades de Certificação Raiz Confiáveis**.




### Use o console Gerenciar Certificados do Computador

1. Abra o console Gerenciar Certificados do Computador e navegar até o repositório de certificados apropriado. Para certificados de servidor, isso é normalmente. **Pessoal** > **Certificados**. Para confiar em um certificado raiz ou autoassinado, escolha **Autoridades de Certificação Raiz Confiáveis** > **Certificados**.
2. Clique com o botão direito do mouse no certificado e selecione > **Todas as Tarefas** > **Importar...**.

   Console Gerenciar Certificados do Computador(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/manage-computer-certificates-console.png)
3. Selecione **Procurar...** e selecione o arquivo.
4. Insira a senha, se necessário.

### Usar PowerShell

Para importar um certificado, use o cmdlet do PowerShell Import-PfxCertificate. Por exemplo, para importar o certificado `certificate.pfx` com a senha `123456` para o armazenamento de certificados pessoal, execute o seguinte comando:

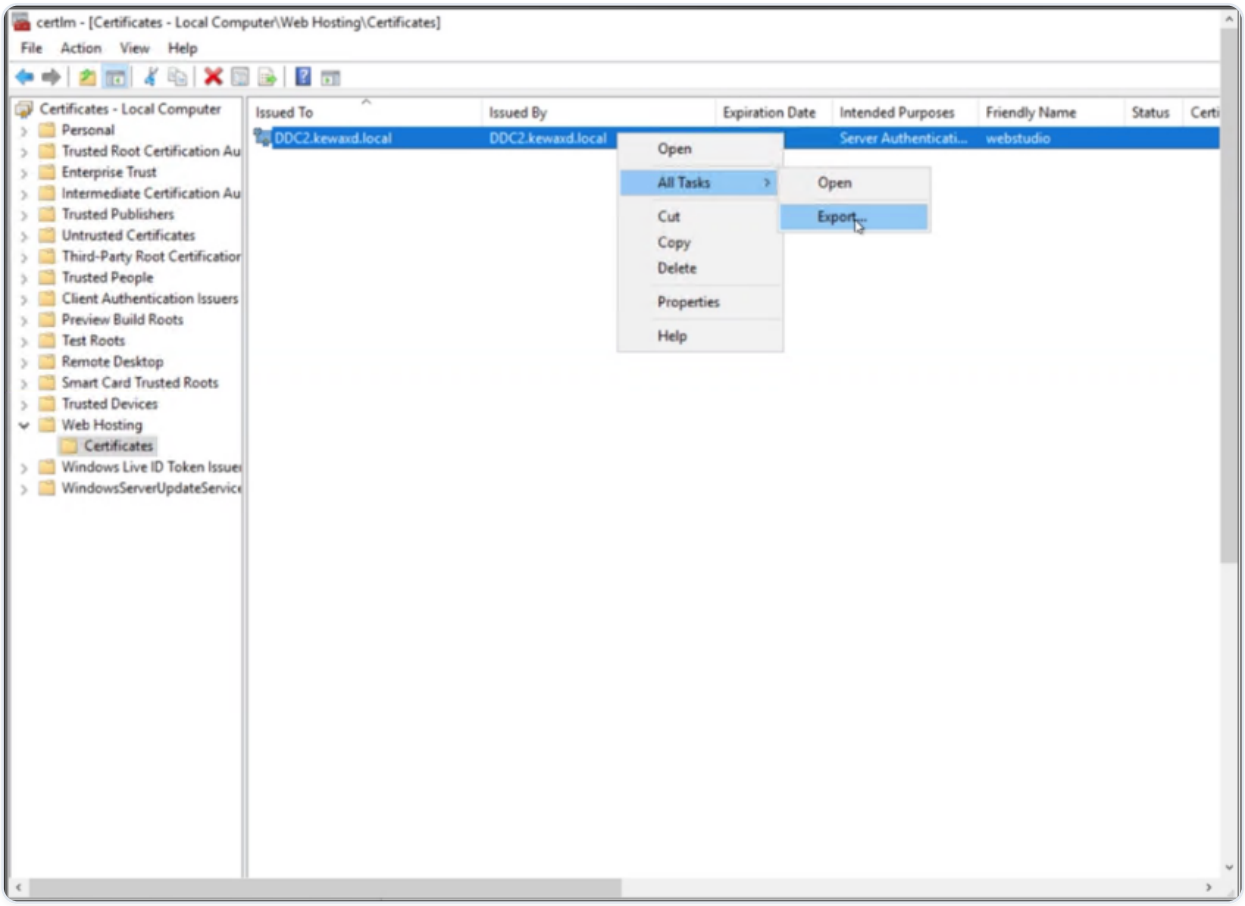
```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

Para importar um certificado raiz confiável, defina o `CertStoreLocation` como `Cert:\LocalMachine\Root\`.

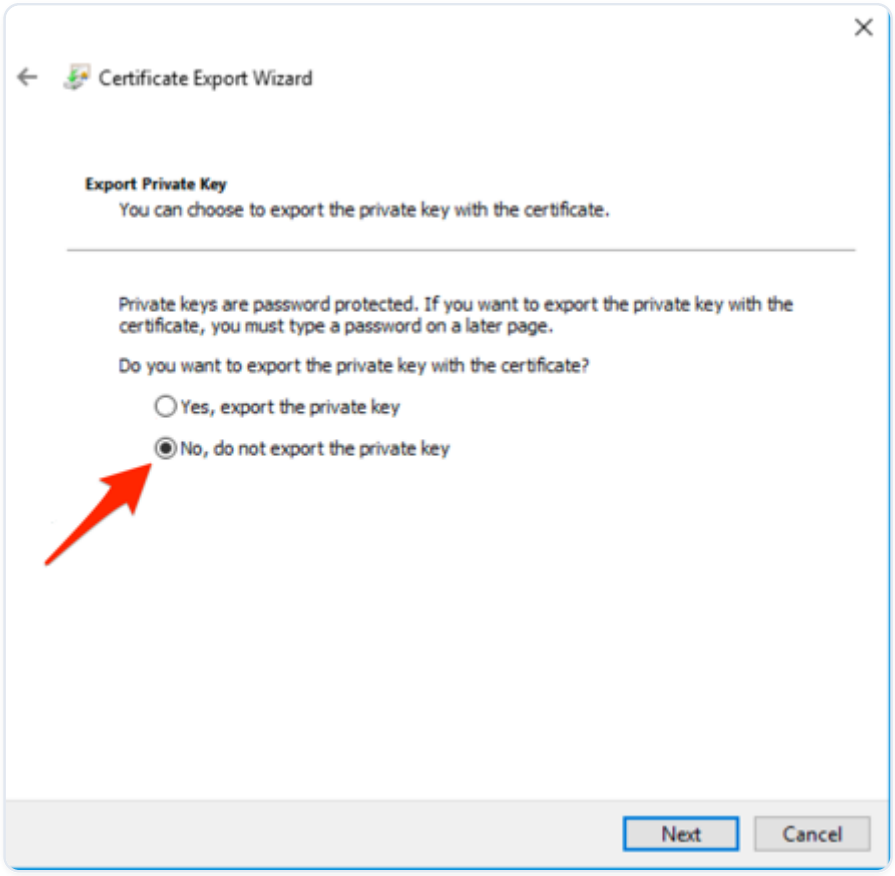
## Exportar certificado sem chave privada

Para exportar um certificado para que você possa importá-lo para outros dispositivos para confiar no certificado, você deve excluir a chave privada.

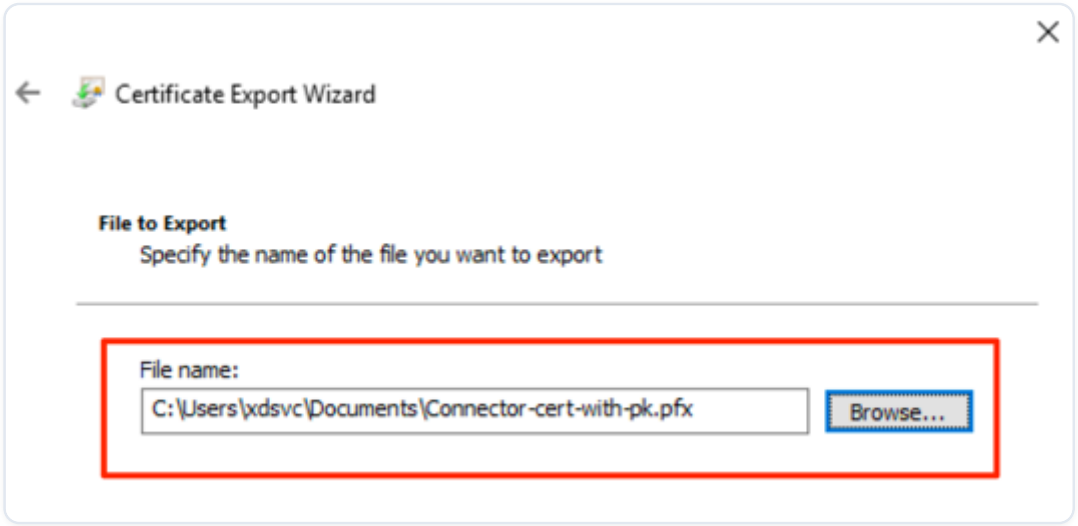
1. Abra o Gerenciar Certificados do Computador. navegar para **Pessoal** > **Certificados** e selecione o certificado que deseja exportar.
2. No menu **Ação**, selecione **Todas as Tarefas** e depois **Exportar**.



3. Escolha **Não, não exportar a chave privada**, e então pressione **Avançar**.




4. Selecione o formato **X.509 binário codificado em DER (.CER)** (o padrão) e pressione **Avançar**.
5. Insira um nome de arquivo e pressione **Avançar**.



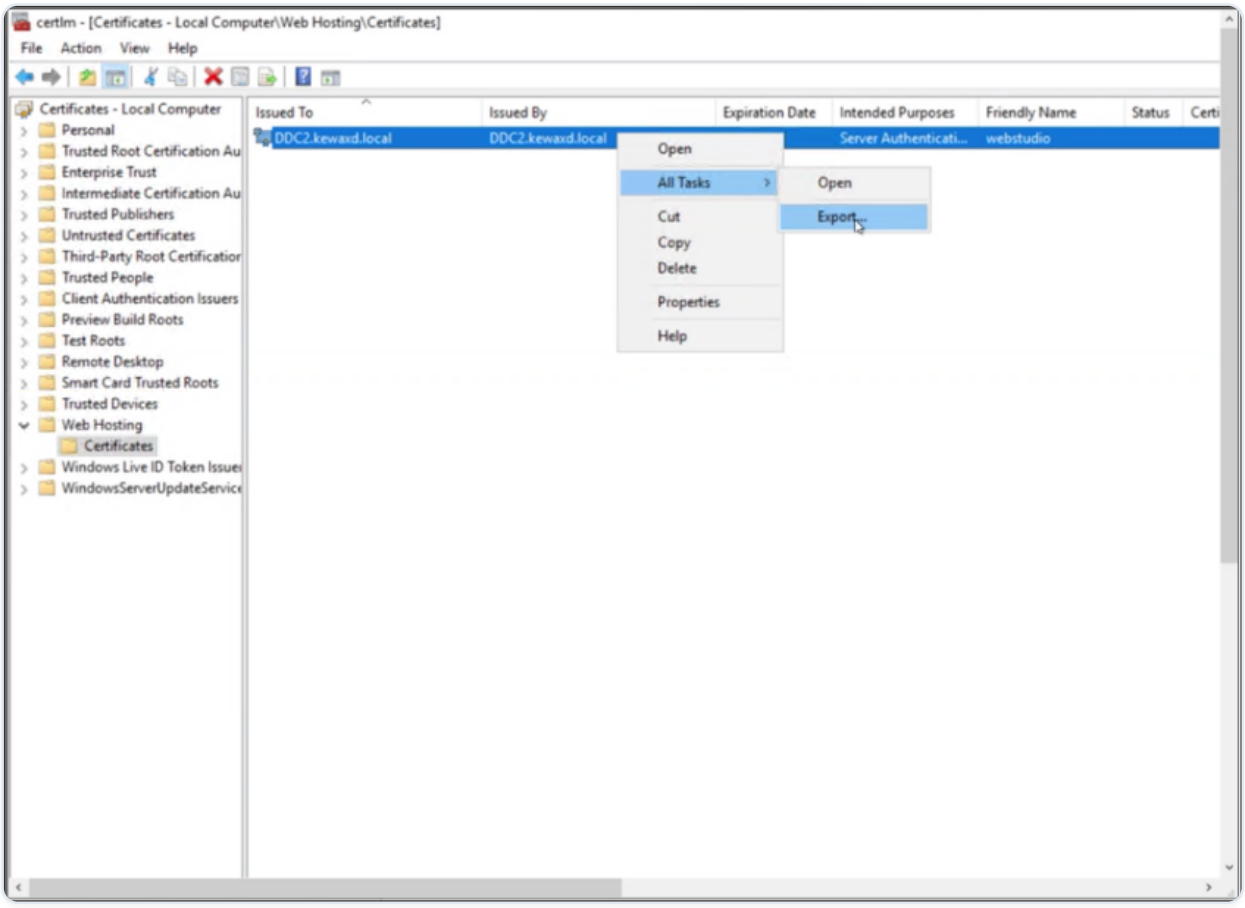

6. Selecione **Concluir**.



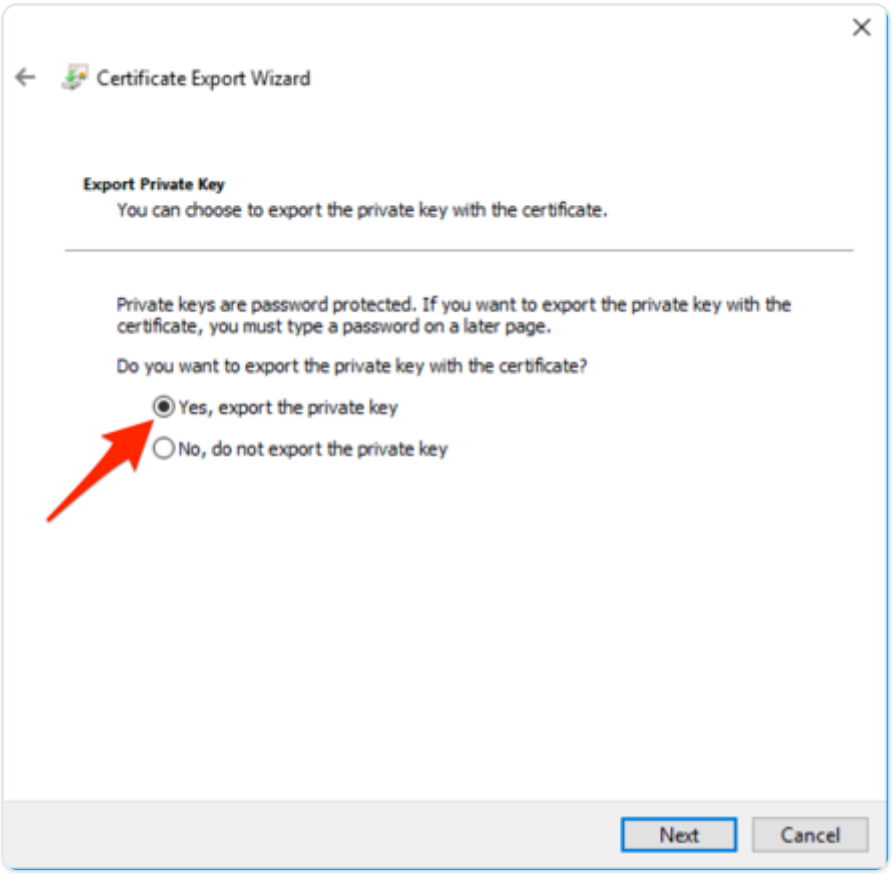

## Exportar certificado com chave privada

Para exportar um certificado para que você possa usá-lo em outros servidores, você deve incluir a chave privada.

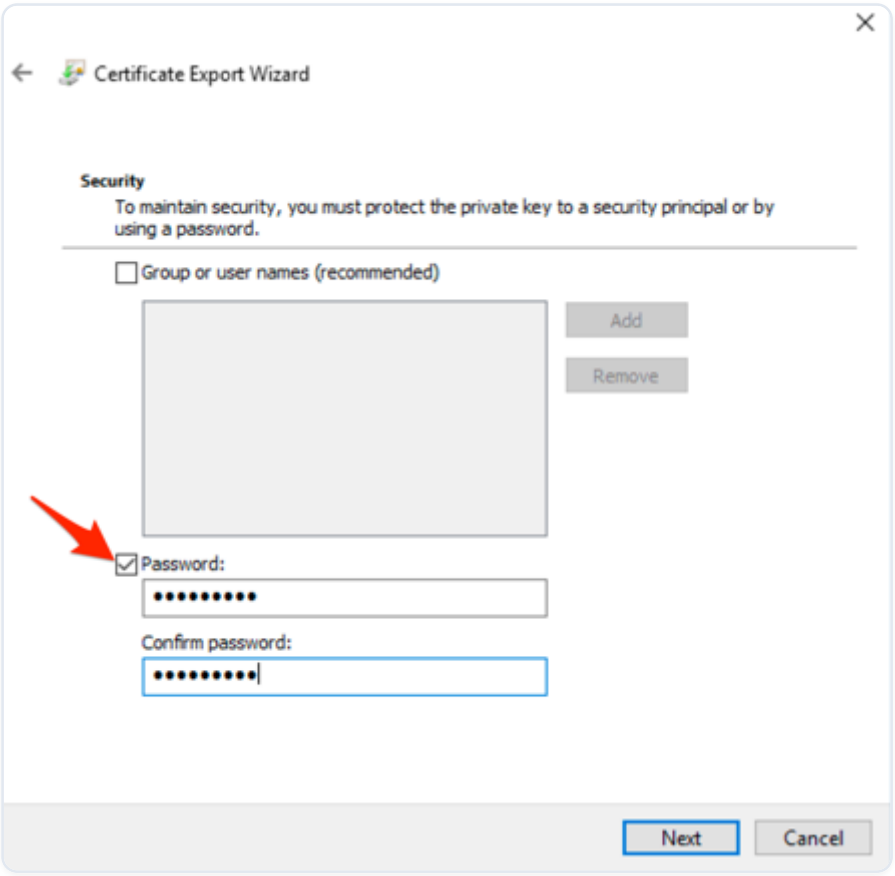
1. Abra o Gerenciar Certificados do Computador. navegar para **Pessoal** > **Certificados** e selecione o certificado que deseja exportar.
2. No menu **Ação**, selecione **Todas as Tarefas** e depois **Exportar**.



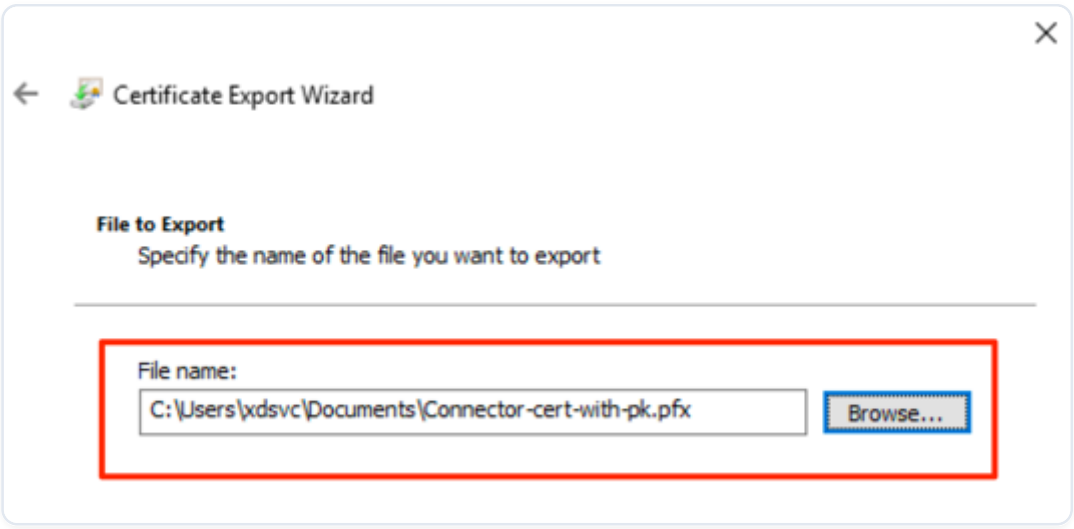

3. Escolha **Sim, exportar a chave privada**, depois selecione **Avançar**.




4. Na guia **Segurança**, digite uma senha e selecione **Avançar**.




5. Digite um nome de arquivo e selecione **Avançar**.




6. Selecione **Concluir**.




## Converter certificado para o formato PEM

Por padrão, o Windows exporta certificados no formato PKCS#12 como um arquivo .pfx que inclui a chave privada. Para usar o certificado em um NetScaler® Gateway ou servidor de licenças, você deve extrair o certificado e as chaves privadas em arquivos separados no formato PEM. Você pode fazer isso usando o openssl.

Para exportar o certificado no formato PEM, execute:

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

Ele solicitará a senha existente e uma nova frase secreta

Para exportar a chave no formato PEM, execute:

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

## Confiando em certificados

- Se você usar um certificado de uma autoridade de certificação pública, os dispositivos normalmente vêm pré-configurados com os certificados raiz.
- Se você usar uma autoridade de certificação corporativa, deverá implantar o certificado raiz em todos os dispositivos que devem confiar nesse certificado. Se estiver usando os Serviços de Certificação do Active Directory, os certificados raiz também serão implantados em todas as

máquinas no domínio usando a Política de Grupo. Você deve importar manualmente o certificado raiz para máquinas que não estão ingressadas no domínio, como seus gateways NetScaler, ou máquinas em outros domínios.

- Se você estiver usando um certificado autoassinado, ele deverá ser instalado manualmente em qualquer máquina que precise confiar no certificado.

Para exportar um certificado raiz autoassinado ou confiável do Windows, consulte exportar certificado sem chave privada.

Para que o Windows confie no certificado, você deve importar o certificado para o armazenamento **Trusted Root Certification Authorities**. Se estiver usando o PowerShell, insira o armazenamento **Cert:\\LocalMachine\Root**.

Para que o NetScaler confie no certificado, primeiro converta o certificado para o formato PEM, depois instale o certificado raiz.

## Cartões inteligentes

Cartões inteligentes e tecnologias equivalentes são suportados dentro das diretrizes descritas neste artigo. Para usar cartões inteligentes com Citrix Virtual Apps ou Citrix Virtual Desktops™:

- Compreenda a política de segurança da sua organização em relação ao uso de cartões inteligentes. Essas políticas podem, por exemplo, indicar como os cartões inteligentes são emitidos e como os usuários devem protegê-los. Alguns aspectos dessas políticas podem precisar ser reavaliados em um ambiente Citrix Virtual Apps™ ou Citrix Virtual Desktops.
- Determine quais tipos de dispositivos de usuário, sistemas operacionais e aplicativos publicados serão usados com cartões inteligentes.
- Familiarize-se com a tecnologia de cartão inteligente e com o hardware e software do fornecedor de cartão inteligente selecionado.
- Saiba como implantar certificados digitais em um ambiente distribuído.

> **Observação:**
>
> O registro de cartão inteligente não é suportado com cartão inteligente rápido. O registro de cartão inteligente pode funcionar quando o cartão inteligente rápido está desabilitado, mas depende do tipo de cartão inteligente e do middleware. Entre em contato com o fornecedor do seu cartão inteligente e middleware para obter informações sobre a integração deles com

> o Citrix Virtual Apps and Desktops e o suporte para registro de cartão inteligente em sessões virtuais.

## Tipos de cartões inteligentes

Cartões inteligentes empresariais e de consumidor têm as mesmas dimensões, conectores elétricos e se encaixam nos mesmos leitores de cartão inteligente.

Cartões inteligentes para uso empresarial contêm certificados digitais. Esses cartões inteligentes suportam o Logon do Windows e também podem ser usados com aplicativos para assinatura digital e criptografia de documentos e e-mails. O Citrix Virtual Apps and Desktops™ suporta esses usos.

Cartões inteligentes para uso do consumidor não contêm certificados digitais; eles contêm um segredo compartilhado. Esses cartões inteligentes podem suportar pagamentos (como um cartão de crédito com chip e assinatura ou chip e PIN). Eles não suportam o Logon do Windows ou aplicativos típicos do Windows. Aplicativos Windows especializados e uma infraestrutura de software adequada (incluindo, por exemplo, uma conexão a uma rede de cartões de pagamento) são necessários para uso com esses cartões inteligentes. Entre em contato com seu representante Citrix para obter informações sobre o suporte a esses aplicativos especializados no Citrix Virtual Apps ou Citrix Virtual Desktops.

Para cartões inteligentes empresariais, existem equivalentes compatíveis que podem ser usados de forma semelhante.

- Um token USB equivalente a um cartão inteligente conecta-se diretamente a uma porta USB. Esses tokens USB geralmente têm o tamanho de um pen drive, mas podem ser tão pequenos quanto um cartão SIM usado em um telefone celular. Eles aparecem como a combinação de um cartão inteligente mais um leitor de cartão inteligente USB.
- Um cartão inteligente virtual usando um Módulo de Plataforma Confiável (TPM) do Windows aparece como um cartão inteligente. Esses cartões inteligentes virtuais são suportados para Windows 8 e Windows 10, usando o aplicativo Citrix Workspace (versão mínima Citrix Receiver 4.3).
    - Versões do Citrix Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) anteriores ao XenApp e XenDesktop 7.6 FP3 não suportam cartões inteligentes virtuais.
    - Para mais informações sobre cartões inteligentes virtuais, consulte Visão geral do cartão inteligente virtual.

> **Nota:** O termo "cartão inteligente virtual" também é usado para descrever um certificado digital armazenado no computador do usuário. Esses certificados digitais não são estritamente equivalentes a cartões inteligentes.

O suporte a cartões inteligentes do Citrix Virtual Apps and Desktops é baseado nas especificações padrão Microsoft Personal Computer/Smart Card (PC/SC). Um requisito mínimo é que os cartões inteligentes e os dispositivos de cartão inteligente devem ser suportados pelo sistema operacional Windows subjacente e devem ser aprovados pelos Microsoft Windows Hardware Quality Labs (WHQL) para serem usados em computadores que executam sistemas operacionais Windows qualificados. Consulte a documentação da Microsoft para obter informações adicionais sobre a conformidade de hardware PC/SC. Outros tipos de dispositivos de usuário podem estar em conformidade com o padrão PS/SC. Para obter mais informações, consulte o programa Citrix Ready.

Geralmente, um driver de dispositivo separado é necessário para o cartão inteligente de cada fornecedor ou equivalente. No entanto, se os cartões inteligentes estiverem em conformidade com um padrão como o NIST Personal Identity Verification (PIV), pode ser possível usar um único driver de dispositivo para uma variedade de cartões inteligentes. O driver de dispositivo deve ser instalado tanto no dispositivo do usuário quanto no Virtual Delivery Agent (VDA). O driver de dispositivo é frequentemente fornecido como parte de um pacote de middleware de cartão inteligente disponível em um parceiro Citrix; o pacote de middleware de cartão inteligente oferece recursos avançados. O driver de dispositivo também pode ser descrito como um Cryptographic Service Provider (CSP), Key Storage Provider (KSP) ou minidriver.

As seguintes combinações de cartão inteligente e middleware para sistemas Windows foram testadas pela Citrix como exemplos representativos de seu tipo. No entanto, outros cartões inteligentes e middleware também podem ser usados. Para mais informações sobre cartões inteligentes e middleware compatíveis com Citrix, consulte `<http://www.citrix.com/ready>`.

| MIDDLEWARE | CARTÕES CORRESPONDENTES |
| --- | --- |
| Mini Driver Gemalto para cartão .NET | Gemalto .NET v2+ |

Para obter informações sobre o uso de cartões inteligentes com outros tipos de dispositivos, consulte a documentação do aplicativo Citrix Workspace™ para esse dispositivo.

## Acesso Remoto a PC

Os cartões inteligentes são suportados apenas para acesso remoto a PCs físicos de escritório que executam Windows 10, Windows 8 ou Windows 7.

Os seguintes cartões inteligentes foram testados com o Acesso Remoto a PC:

| MIDDLEWARE | CARTÕES CORRESPONDENTES |
| --- | --- |
| Minidriver Gemalto .NET | Gemalto .NET v2+ |

## Cartão inteligente rápido

O cartão inteligente rápido é uma melhoria em relação ao redirecionamento de cartão inteligente baseado em HDX PC/SC existente. Ele melhora o desempenho quando cartões inteligentes são usados em situações de WAN de alta latência. Quando a latência é alta, a melhoria de desempenho pode ser significativa (por exemplo, 15 segundos para um logon de cartão inteligente rápido do Windows versus mais de 1 minuto com o redirecionamento de cartão inteligente baseado em PC/SC).

O cartão inteligente rápido é habilitado por padrão em máquinas host com VDAs Windows atualmente suportados. Para desabilitar o Cartão Inteligente Rápido no lado do host — por exemplo, para fins de diagnóstico — defina a configuração de registro 'Disable Cryptographic Redirection' para qualquer valor diferente de zero:

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

No lado do cliente, para habilitar o cartão inteligente rápido, inclua o parâmetro ICA SmartCardCryptographicRedirection no arquivo *default.ica* do site StoreFront associado:

```
[WFClient]

SmartCardCryptographicRedirection=On
```

Além disso, no lado do cliente, o cartão inteligente rápido pode ser forçado a ser habilitado ou forçado a ser desabilitado (por exemplo, para fins de diagnóstico) com as seguintes configurações de registro:

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (como um DWORD diferente de zero)

Ou

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (como um DWORD diferente de zero)

O hive de registro de 32 bits deve ser especificado (usando `WOW6432Node`) se a máquina cliente for de 64 bits.

Limitações:

- Apenas o aplicativo Citrix Workspace para Windows suporta cartão inteligente rápido. Se você configurar cartões inteligentes rápidos no arquivo default.ica, os aplicativos Citrix Workspace que não são para Windows ainda usarão o redirecionamento PC/SC existente.
- Os únicos cenários de salto duplo que o cartão inteligente rápido suporta são ICA® > ICA com cartão inteligente rápido habilitado em ambos os saltos. Como o cartão inteligente rápido não suporta cenários de salto duplo ICA > RDP, esses cenários não funcionam.
- O cartão inteligente rápido não suporta Criptografia de Próxima Geração. Assim, o cartão inteligente rápido não suporta cartões inteligentes de Criptografia de Curva Elíptica (ECC).
- O cartão inteligente rápido suporta apenas operações de contêiner de chave somente leitura.
- O cartão inteligente rápido não suporta a alteração do PIN do cartão inteligente.

A partir do VDA versão 2203 e do aplicativo Citrix Workspace versão 2202 para Windows (ou posterior), o cartão inteligente rápido é compatível com a Criptografia de Próxima Geração (CNG). Além disso, cartões inteligentes de Criptografia de Curva Elíptica (ECC) são suportados com as seguintes curvas: P-256, P-384, P-521 bits, para ECDSA e ECDH.

A partir da versão 2203 do VDA, o cartão inteligente rápido adiciona a capacidade de armazenar em cache o PIN do cartão inteligente entre os aplicativos da mesma sessão de logon do usuário. Por exemplo, se o **Cache de PIN da Sessão** estiver ativado e o usuário final tiver fornecido anteriormente o PIN do cartão inteligente ao Outlook, quando o Word for usado para assinar um documento, o Word usará o PIN do cartão inteligente já armazenado em cache (enviado ao Outlook). O **Cache de PIN da Sessão** melhora a experiência do usuário, reduzindo o número de vezes que o usuário precisa inserir o PIN do cartão inteligente. Além disso, se o cartão inteligente for usado para fazer logon no VDA, o PIN de logon do cartão inteligente do Windows pode ser opcionalmente salvo no **Cache de PIN da Sessão**. Isso pode melhorar ainda mais a experiência do usuário.

O **Cache de PIN da Sessão** é desativado por padrão. Ele pode ser ativado e controlado com as seguintes configurações de registro no VDA:

Em HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` como um DWORD (não zero para habilitar)
- `EnableLogonPinSessionCache` como um DWORD (não zero para habilitar)
- `PinSessionCacheEntryStaleTimeout` como um DWORD (número de segundos antes que uma entrada se torne obsoleta, o padrão é 1 hora)

## Tipos de leitores de cartão inteligente

Um leitor de cartão inteligente pode ser integrado ao dispositivo do usuário ou anexado separadamente ao dispositivo do usuário (geralmente via USB ou Bluetooth). Leitores de cartão de contato que estão em conformidade com a especificação USB Chip/Smart Card Interface Devices (CCID) são suportados. Eles contêm um slot ou passagem no qual o usuário insere o cartão inteligente. O padrão Deutsche Kreditwirtschaft (DK) define quatro classes de leitores de cartão de contato.

- Os leitores de cartão inteligente Classe 1 são os mais comuns e geralmente contêm um slot. Os leitores de cartão inteligente Classe 1 são suportados, geralmente com um driver de dispositivo CCID padrão fornecido com o sistema operacional.
- Os leitores de cartão inteligente Classe 2 também contêm um teclado seguro que não pode ser acessado pelo dispositivo do usuário. Os leitores de cartão inteligente Classe 2 podem ser integrados a um teclado com um teclado seguro integrado. Para leitores de cartão inteligente Classe 2, entre em contato com seu representante Citrix; um driver de dispositivo específico do leitor pode ser necessário para habilitar a capacidade do teclado seguro.
- Os leitores de cartão inteligente Classe 3 também contêm um display seguro. Os leitores de cartão inteligente Classe 3 não são suportados.
- Os leitores de cartão inteligente Classe 4 também contêm um módulo de transação seguro. Os leitores de cartão inteligente Classe 4 não são suportados.

> **Observação:**
>
> A classe do leitor de cartão inteligente não está relacionada à classe de dispositivo USB.
>
> Os leitores de cartão inteligente devem ser instalados com um driver de dispositivo correspondente no dispositivo do usuário.

Para obter informações sobre leitores de cartão inteligente suportados, consulte a documentação do aplicativo Citrix Workspace que você está usando. Na documentação do aplicativo Citrix

Workspace, as versões suportadas são listadas em um artigo sobre cartão inteligente ou no artigo de requisitos do sistema.

## Experiência do usuário

O suporte a cartões inteligentes é integrado ao Citrix Virtual Apps and Desktops, usando um canal virtual de cartão inteligente ICA/HDX específico que é habilitado por padrão.

Importante: Não use o redirecionamento USB genérico para leitores de cartão inteligente. Isso é desabilitado por padrão para leitores de cartão inteligente e não é suportado se habilitado.

Vários cartões inteligentes e vários leitores podem ser usados no mesmo dispositivo do usuário, mas se a autenticação pass-through estiver em uso, apenas um cartão inteligente deve ser inserido quando o usuário inicia um desktop ou aplicativo virtual. Quando um cartão inteligente é usado dentro de um aplicativo (por exemplo, para funções de assinatura digital ou criptografia), pode haver outros prompts para inserir um cartão inteligente ou digitar um PIN. Isso pode ocorrer se mais de um cartão inteligente tiver sido inserido ao mesmo tempo.

- Se os usuários forem solicitados a inserir um cartão inteligente quando o cartão inteligente já estiver no leitor, eles devem selecionar Cancelar.
- Se os usuários forem solicitados a inserir o PIN, eles devem inseri-lo novamente.

Você pode redefinir PINs usando um sistema de gerenciamento de cartão ou um utilitário do fornecedor.

> **Importante:**

> Dentro de uma sessão do Citrix Virtual Apps ou Citrix Virtual Desktops, o uso de um cartão inteligente com o aplicativo Microsoft Remote Desktop Connection não é suportado. Isso às vezes é descrito como um uso de "salto duplo".

## Antes de implantar cartões inteligentes

- Obtenha um driver de dispositivo para o leitor de cartão inteligente e instale-o no dispositivo do usuário. Muitos leitores de cartão inteligente podem usar o driver de dispositivo CCID fornecido pela Microsoft.
- Obtenha um driver de dispositivo e software de provedor de serviços criptográficos (CSP) do seu fornecedor de cartão inteligente e instale-os em dispositivos de usuário e desktops virtuais. O driver e o software CSP devem ser compatíveis com o Citrix Virtual Apps and

Desktops; verifique a documentação do fornecedor para compatibilidade. Para desktops virtuais que usam cartões inteligentes que suportam e usam o modelo de minidriver, os minidrivers de cartão inteligente são baixados automaticamente, mas você também pode obtê-los em http://catalog.update.microsoft.com ou de seu fornecedor. Além disso, se o middleware PKCS#11 for necessário, obtenha-o do fornecedor do cartão.

- Importante: A Citrix recomenda que você instale e teste os drivers e o software CSP em um computador físico antes de instalar o software Citrix.
- Adicione a URL do Citrix Receiver™ for Web à lista de Sites Confiáveis para usuários que usam cartões inteligentes no Internet Explorer com Windows 10. No Windows 10, o Internet Explorer não é executado no modo protegido por padrão para sites confiáveis.
- Certifique-se de que sua infraestrutura de chave pública (PKI) esteja configurada adequadamente. Isso inclui garantir que o mapeamento de certificado para conta esteja configurado corretamente para o ambiente do Active Directory e que a validação do certificado do usuário possa ser realizada com sucesso.
- Certifique-se de que sua implantação atenda aos requisitos de sistema dos outros componentes Citrix usados com cartões inteligentes, incluindo o aplicativo Citrix Workspace e o StoreFront.
- Garanta o acesso aos seguintes servidores em seu Site:
  - O controlador de domínio do Active Directory para a conta de usuário que está associada a um certificado de logon no cartão inteligente
  - Delivery Controller™
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Opcional para Acesso Remoto a PC): Microsoft Exchange Server

## Habilitar o uso de cartão inteligente

**Etapa 1.** Emita cartões inteligentes para os usuários de acordo com sua política de emissão de cartões.

**Etapa 2.** (Opcional) Configure os cartões inteligentes para habilitar os usuários para Acesso Remoto a PC.

**Passo 3.** Instale e configure o Delivery Controller e o StoreFront (se ainda não estiverem instalados) para o acesso remoto de cartão inteligente.

**Etapa 4.** Habilite o StoreFront para o uso de cartão inteligente. Para obter detalhes, consulte Configurar a autenticação de cartão inteligente na documentação do StoreFront.

**Etapa 5.** Habilite o Citrix Gateway/Access Gateway para o uso de cartão inteligente. Para obter detalhes, consulte Configurando Autenticação e Autorização e Configurando Acesso a Cartão Inteligente com a Interface Web na documentação do NetScaler.

**Etapa 6.** Habilite VDAs para o uso de cartão inteligente.

- Certifique-se de que o VDA tenha os aplicativos e atualizações necessários.
- Instale o middleware.
- Configure o acesso remoto de cartão inteligente, habilitando a comunicação de dados do cartão inteligente entre o aplicativo Citrix Workspace em um dispositivo de usuário e uma sessão de desktop virtual.

**Etapa 7.** Habilite os dispositivos do usuário (incluindo máquinas ingressadas no domínio ou não ingressadas no domínio) para o uso de cartão inteligente. Consulte Configurar a autenticação de cartão inteligente na documentação do StoreFront para obter detalhes.

- Importe o certificado raiz da autoridade de certificação e o certificado da autoridade de certificação emissora para o keystore do dispositivo.
- Instale o middleware de cartão inteligente do seu fornecedor.
- Instale e configure o aplicativo Citrix Workspace para Windows, certificando-se de importar icaclient.adm usando o Console de Gerenciamento de Política de Grupo e habilitar a autenticação por cartão inteligente.

**Passo 8.** Teste a implantação. Certifique-se de que a implantação esteja configurada corretamente, iniciando um desktop virtual com o cartão inteligente de um usuário de teste. Teste todos os mecanismos de acesso possíveis (por exemplo, acessando o desktop através do Internet Explorer e do aplicativo Citrix Workspace).

## Rastrear contagem de inserções do leitor de cartão inteligente

Com o acesso remoto de cartão inteligente, você pode rastrear o número de vezes que um cartão inteligente foi inserido ou removido de um leitor usando a função SCardGetStatusChange. A função atualiza um array de estruturas de dados SCARD_READERSTATE — uma para cada leitor que você monitora. A palavra alta (16 bits) do campo dwEventState de cada SCARD_READERSTATE contém a contagem do leitor. Para mais informações, consulte os artigos da Microsoft SCardGetStatusChangeA function e SCARD_READERSTATEA structure.

A configuração **Relatório de Contagem de Inserções do Leitor** está desabilitada por padrão. Para habilitar o rastreamento, adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Nome: EnableReaderInsertCountReporting

Tipo: DWORD

Valor: Qualquer valor diferente de zero

Quando a sessão é desconectada, a contagem é redefinida para zero.

**Relatório de Contagem de Inserções do Leitor** é compatível com middleware de cartão inteligente de terceiros.

## Implantações de smart card

Os seguintes tipos de implantações de smart card são suportados por esta versão do produto e por ambientes mistos que contêm esta versão. Outras configurações podem funcionar, mas não são suportadas.

| TIPO | CONECTIVIDADE DO STOREFRONT™ |
|---|---|
| Computadores locais ingressados no domínio | Conectado diretamente |
| Acesso remoto de computadores ingressados no domínio | Conectado via Citrix Gateway |
| Computadores não ingressados no domínio | Conectado diretamente |
| Acesso remoto de computadores não ingressados no domínio | Conectado via Citrix Gateway |
| Computadores não ingressados no domínio e thin clients acessando o site do Desktop Appliance | Conectado via sites do Desktop Appliance |
| Computadores ingressados no domínio e thin clients acessando o StoreFront através da URL dos Serviços XenApp® | Conectado via URLs dos Serviços XenApp |

Os tipos de implantação são definidos pelas características do dispositivo do usuário ao qual o leitor de cartão inteligente está conectado:

- Se o dispositivo está associado a um domínio ou não.
- Como o dispositivo está conectado ao StoreFront.
- Qual software é usado para visualizar desktops e aplicativos virtuais.

Além disso, aplicativos habilitados para cartão inteligente, como Microsoft Word e Microsoft Excel, podem ser usados nessas implantações. Esses aplicativos permitem que os usuários assinem digitalmente ou criptografem documentos.

### Autenticação bimodal

Sempre que possível em cada uma dessas implantações, o Receiver oferece suporte à autenticação bimodal, oferecendo ao usuário a escolha entre usar um cartão inteligente e inserir seu nome de usuário e senha. Isso é útil se o cartão inteligente não puder ser usado (por exemplo, o usuário o deixou em casa ou o certificado de logon expirou).

Como os usuários de dispositivos não associados a um domínio fazem logon diretamente no Receiver para Windows, você pode permitir que os usuários recorram à autenticação explícita. Se você configurar a autenticação bimodal, os usuários serão inicialmente solicitados a fazer logon usando seus cartões inteligentes e PINs, mas terão a opção de selecionar a autenticação explícita se tiverem algum problema com seus cartões inteligentes.

Se você implantar o Citrix Gateway, os usuários farão logon em seus dispositivos e serão solicitados pelo Receiver para Windows a autenticar no Citrix Gateway. Isso se aplica a dispositivos associados a domínio e não associados a domínio. Os usuários podem fazer logon no Citrix Gateway usando seus cartões inteligentes e PINs, ou com credenciais explícitas. Isso permite que você forneça aos usuários autenticação bimodal para logons do Citrix Gateway. Configure a autenticação pass-through do Citrix Gateway para o StoreFront e delegue a validação de credenciais ao Citrix Gateway para usuários de cartão inteligente, para que os usuários sejam autenticados silenciosamente no StoreFront.

### Considerações sobre várias florestas do Active Directory

Em um ambiente Citrix, os cartões inteligentes são suportados em uma única floresta. Logons de cartão inteligente entre florestas exigem uma confiança de floresta bidirecional direta para todas as contas de usuário. Implantações multifloresta mais complexas envolvendo cartões inteligentes (ou seja, onde as confianças são apenas unidirecionais ou de tipos diferentes) não são suportadas.

Você pode usar cartões inteligentes em um ambiente Citrix que inclui desktops remotos. Esse recurso pode ser instalado localmente (no dispositivo do usuário ao qual o cartão inteligente está conectado) ou remotamente (no desktop remoto ao qual o dispositivo do usuário se conecta).

### Política de remoção de cartão inteligente

A política de remoção de cartão inteligente definida no produto determina o que acontece se você remover o cartão inteligente do leitor durante uma sessão. A política de remoção de cartão inteligente é configurada e gerenciada pelo sistema operacional Windows.

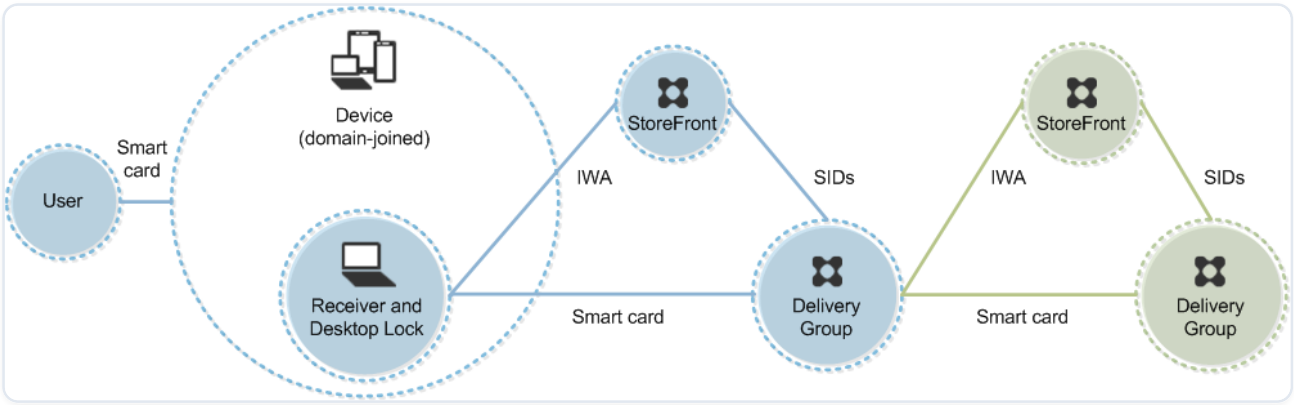
| CONFIGURAÇÃO DA POLÍTICA | COMPORTAMENTO DA ÁREA DE TRABALHO |
|---|---|
| Nenhuma ação | Nenhuma ação. |
| Bloquear estação de trabalho | A sessão da área de trabalho é desconectada e a área de trabalho virtual é bloqueada. |
| Forçar logoff | O usuário é forçado a fazer logoff. Se a conexão de rede for perdida e essa configuração estiver ativada, a sessão poderá ser desconectada e o usuário poderá perder dados. |
| Desconectar se for uma sessão remota do Terminal Services | A sessão é desconectada e a área de trabalho virtual é bloqueada. |

### Verificação de revogação de certificado

Se a verificação de revogação de certificado estiver ativada e um usuário inserir um cartão inteligente com um certificado inválido em um leitor de cartão, o usuário não poderá autenticar ou acessar a área de trabalho ou o aplicativo relacionado ao certificado. Por exemplo, se o certificado inválido for usado para descriptografia de e-mail, o e-mail permanecerá criptografado. Se outros certificados no cartão, como os usados para autenticação, ainda forem válidos, essas funções permanecerão ativas.

### Exemplo de implantação: computadores ingressados no domínio

Esta implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.

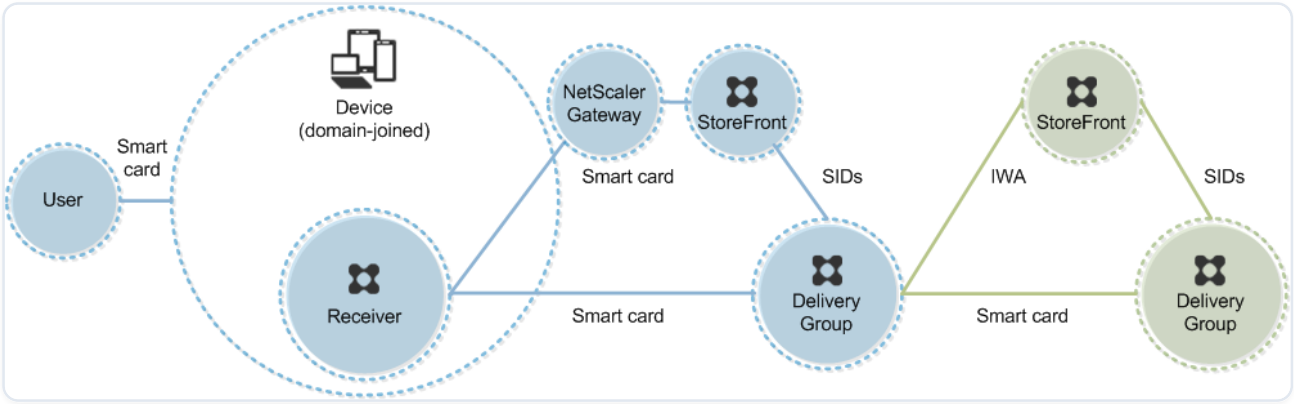



Um usuário faz logon em um dispositivo usando um cartão inteligente e um PIN. O Receiver autentica o usuário em um servidor StoreFront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia uma área de trabalho virtual ou um aplicativo, ele não é solicitado a inserir um PIN novamente porque o recurso de logon único está configurado no Receiver.

Esta implantação pode ser estendida para um double-hop com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro hop pode ser reutilizada no segundo hop ou usada apenas no segundo hop.

### Exemplo de implantação: acesso remoto de computadores ingressados no domínio

Esta implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam ao StoreFront através do Citrix Gateway/Access Gateway.



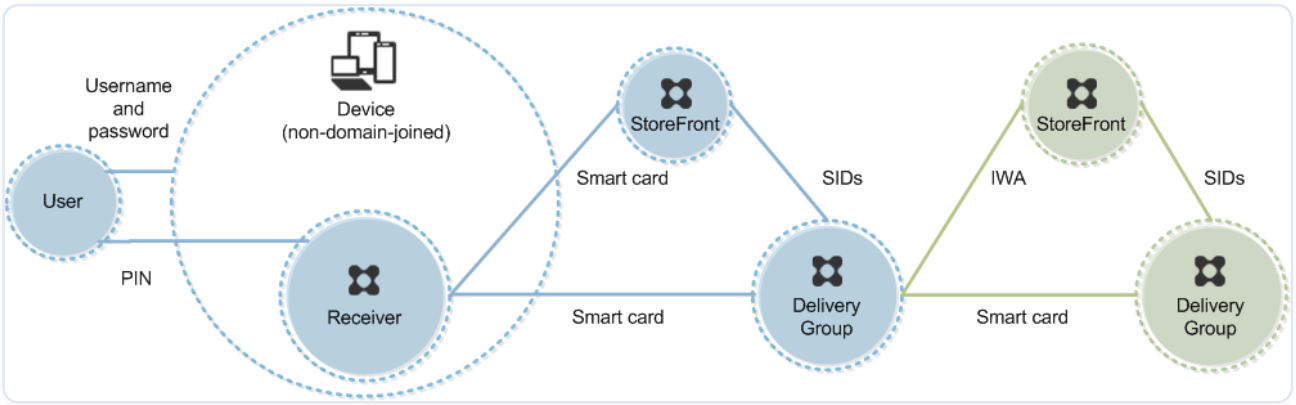

Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN e, em seguida, faz logon novamente no Citrix Gateway/Access Gateway. Este segundo logon pode ser feito com o cartão inteligente e PIN ou com um nome de usuário e senha, pois o Receiver permite autenticação bimodal nesta implantação.

O usuário é automaticamente conectado ao StoreFront, que passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps™ ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual ou aplicativo, ele não é solicitado novamente a inserir um PIN porque o recurso de logon único está configurado no Receiver.

Esta implantação pode ser estendida para um double-hop com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro hop pode ser reutilizada no segundo hop ou usada apenas no segundo hop.

### Exemplo de implantação: computadores não ingressados no domínio

Esta implantação envolve dispositivos de usuário não ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.



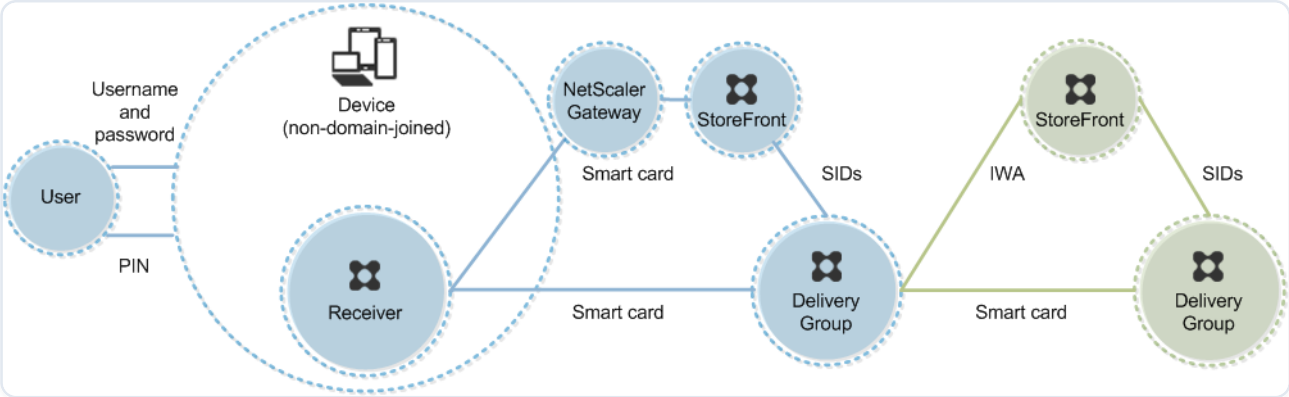

Um usuário faz logon em um dispositivo. Normalmente, o usuário insere um nome de usuário e senha, mas, como o dispositivo não está ingressado em um domínio, as credenciais para este logon são opcionais. Como a autenticação bimodal é possível nesta implantação, o Receiver solicita ao usuário um cartão inteligente e PIN ou um nome de usuário e senha. O Receiver então autentica-se no StoreFront.

O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual ou aplicativo, ele é solicitado novamente a inserir um PIN porque o recurso de logon único não está disponível nesta implantação.

Esta implantação pode ser estendida para um double-hop com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro hop pode ser reutilizada no segundo hop ou usada apenas no segundo hop.

### Exemplo de implantação: acesso remoto de computadores não ingressados no domínio

Esta implantação envolve dispositivos de usuário não associados a domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.




Um usuário faz logon em um dispositivo. Normalmente, o usuário insere um nome de usuário e senha, mas, como o dispositivo não está associado a um domínio, as credenciais para este logon são opcionais. Como a autenticação bimodal é possível nesta implantação, o Receiver solicita ao usuário um cartão inteligente e PIN ou um nome de usuário e senha. O Receiver então se autentica no Storefront.

O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop ou aplicativo virtual, o usuário é solicitado a inserir um PIN novamente porque o recurso de logon único não está disponível nesta implantação.

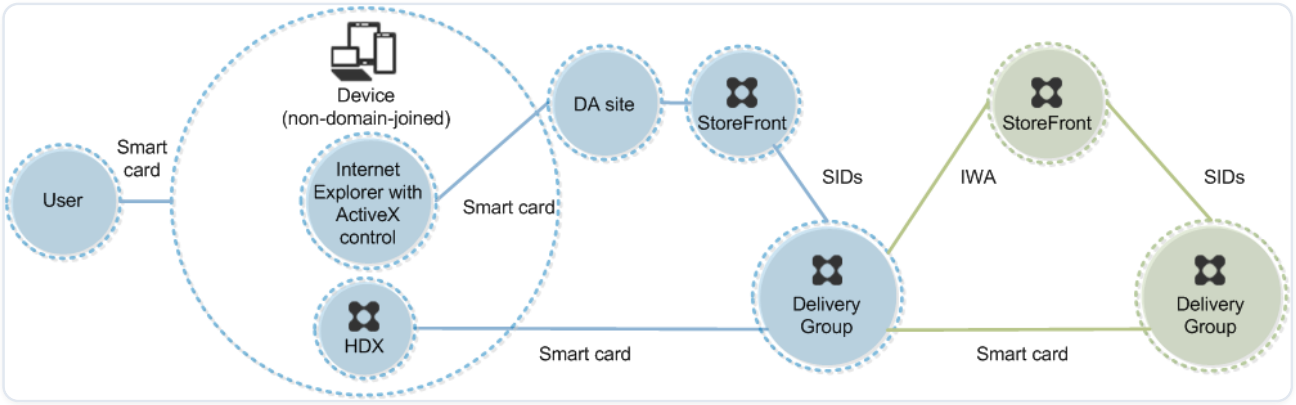
Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

### Exemplo de implantação: computadores não associados a domínio e thin clients acessando o site do Desktop Appliance

Esta implantação envolve dispositivos de usuário não associados a domínio que podem executar o Desktop Lock e se conectar ao StoreFront por meio de sites do Desktop Appliance.

O Desktop Lock é um componente separado que é lançado com o Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. É uma alternativa ao Desktop Viewer e foi projetado principalmente para computadores Windows reaproveitados e thin clients Windows. O Desktop Lock substitui o shell do Windows e o Gerenciador de Tarefas nesses dispositivos de usuário, impedindo que os

usuários acessem os dispositivos subjacentes. Com o Desktop Lock, os usuários podem acessar desktops de Máquina de Servidor Windows e desktops de Máquina de Desktop Windows. A instalação do Desktop Lock é opcional.



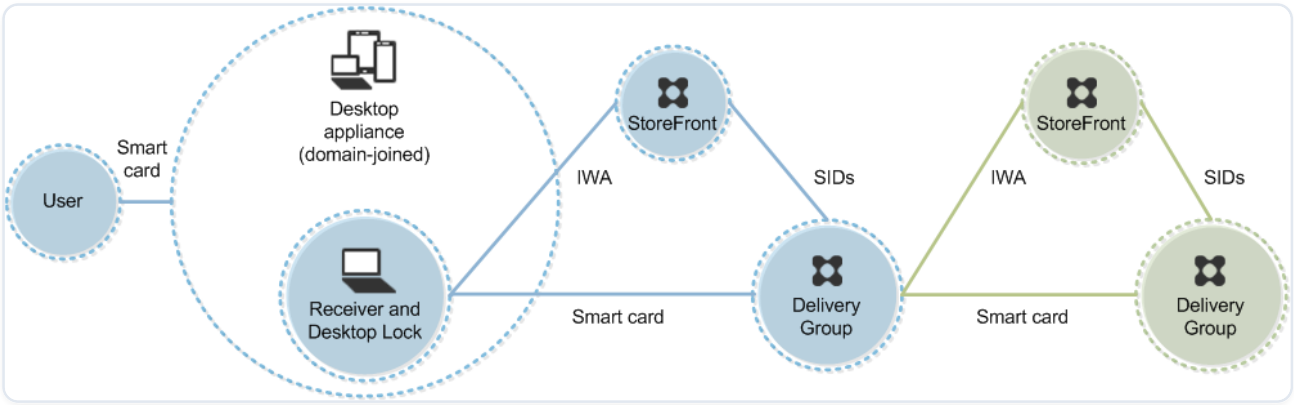

Um usuário faz logon em um dispositivo com um cartão inteligente. Se o Desktop Lock estiver em execução no dispositivo, o dispositivo será configurado para iniciar um site do Desktop Appliance por meio do Internet Explorer em execução no Modo Quiosque. Um controle ActiveX no site solicita ao usuário um PIN e o envia ao StoreFront. O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. O primeiro desktop disponível na lista alfabética em um Grupo de Desktops atribuído é iniciado.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

### Exemplo de implantação: computadores associados a domínio e thin clients acessando o StoreFront por meio da URL dos Serviços XenApp

Esta implantação envolve dispositivos de usuário associados a domínio que executam o Desktop Lock e se conectam ao StoreFront por meio de URLs dos Serviços XenApp.

O Desktop Lock é um componente separado que é lançado com o Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. É uma alternativa ao Desktop Viewer e foi projetado principalmente para computadores Windows reaproveitados e thin clients Windows. O Desktop Lock substitui o shell do Windows e o Gerenciador de Tarefas nesses dispositivos de usuário, impedindo que os usuários acessem os dispositivos subjacentes. Com o Desktop Lock, os usuários podem acessar desktops de Máquina de Servidor Windows e desktops de Máquina de Desktop Windows. A instalação do Desktop Lock é opcional.




Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN. Se o Desktop Lock estiver em execução no dispositivo, ele autentica o usuário em um servidor Storefront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual, o usuário não é solicitado a inserir um PIN novamente porque o recurso de logon único está configurado no Receiver.

Este tipo de implantação pode ser estendido para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

## Autenticação pass-through e logon único com cartões inteligentes

### Autenticação pass-through

A autenticação pass-through com cartões inteligentes para desktops virtuais é suportada em dispositivos de usuário que executam Windows 10, Windows 8 e Windows 7 SP1 Enterprise e Professional Editions.

A autenticação pass-through com cartões inteligentes para aplicativos hospedados é suportada em servidores que executam Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 e Windows Server 2008 R2 SP1.

Para usar a autenticação pass-through com aplicativos hospedados por cartões inteligentes, certifique-se de habilitar o uso do Kerberos ao configurar o Pass-through com cartão inteligente como método de autenticação para o site.

Nota: A disponibilidade da autenticação pass-through com cartões inteligentes depende de muitos fatores, incluindo, mas não se limitando a:

- As políticas de segurança da sua organização em relação à autenticação pass-through.

- Tipo e configuração do middleware.
- Tipos de leitores de cartão inteligente.
- Política de cache de PIN do middleware.

A autenticação pass-through com cartões inteligentes é configurada no Citrix StoreFront. Consulte a documentação do StoreFront para obter detalhes.

### Logon único

O logon único é um recurso da Citrix que implementa a autenticação pass-through com inicializações de aplicativos e desktops virtuais. Você pode usar esse recurso em implantações de cartão inteligente ingressadas no domínio, diretas para o StoreFront e ingressadas no domínio, NetScaler para StoreFront para reduzir o número de vezes que os usuários inserem seu PIN. Para usar o logon único nesses tipos de implantação, edite os seguintes parâmetros no arquivo default.ica, que está localizado no servidor StoreFront:

- Implantações de cartão inteligente ingressadas no domínio, diretas para o StoreFront — Defina DisableCtrlAltDel como Off
- Implantações de cartão inteligente ingressadas no domínio, NetScaler para StoreFront — Defina UseLocalUserAndPassword como On

Para mais instruções sobre como definir esses parâmetros, consulte a documentação do StoreFront ou do Citrix Gateway.

A disponibilidade da funcionalidade de logon único depende de muitos fatores, incluindo, mas não se limitando a:

- As políticas de segurança da sua organização em relação ao logon único.
- Tipo e configuração do middleware.
- Tipos de leitores de cartão inteligente.
- Política de cache de PIN do middleware.

> **Nota:**

> Quando um usuário faz logon no Virtual Delivery Agent (VDA) em uma máquina com um leitor de cartão inteligente conectado, um bloco do Windows pode aparecer representando o modo de autenticação bem-sucedido anterior, como cartão inteligente ou senha. Como resultado, quando o logon único está habilitado, o bloco de logon único pode aparecer. Para

> fazer logon, o usuário deve selecionar **Trocar Usuários** para selecionar outro bloco, pois o bloco de logon único não funcionará.

# Segurança da Camada de Transporte (TLS)

O Citrix Virtual Apps e Desktops suporta o protocolo Transport Layer Security (TLS) para conexões baseadas em TCP entre componentes. O Citrix Virtual Apps e Desktops também suporta o protocolo Datagram Transport Layer Security (DTLS) para conexões ICA/HDX baseadas em UDP, usando transporte adaptável.

TLS e DTLS são semelhantes e suportam os mesmos certificados digitais. A configuração de um Site do Citrix Virtual Apps ou Citrix Virtual Desktops™ para usar TLS também o configura para usar DTLS. Use os seguintes procedimentos; as etapas são comuns a TLS e DTLS, exceto onde indicado:

- Obtenha, instale e registre um certificado de servidor em todos os Delivery Controllers e configure uma porta com o certificado TLS. Para obter detalhes, consulte Instalar certificados de servidor TLS nos Controllers.

  Opcionalmente, você pode alterar as portas que o Controller usa para escutar o tráfego HTTP e HTTPS.
- Habilite conexões TLS entre o aplicativo Citrix Workspace™ e os Virtual Delivery Agents (VDAs) concluindo as seguintes tarefas:
  - Configure o TLS nas máquinas onde os VDAs estão instalados. (Para sua conveniência, referências futuras a máquinas onde os VDAs estão instalados são simplesmente chamadas de "VDAs".) Para informações gerais, consulte Configurações de TLS em VDAs. É altamente recomendável que você use o script PowerShell fornecido pela Citrix para configurar TLS/DTLS. Para obter detalhes, consulte Configurar TLS em um VDA usando o script PowerShell. No entanto, se você quiser configurar TLS/DTLS manualmente, consulte Configurar TLS em um VDA manualmente.
  - Configure o TLS nos Delivery Groups que contêm os VDAs executando um conjunto de cmdlets PowerShell no Studio. Para obter detalhes, consulte Configurar TLS em Delivery Groups.

    Requisitos e considerações:

    - A habilitação de conexões TLS entre usuários e VDAs é válida apenas para Sites do XenApp 7.6 e XenDesktop 7.6, além de versões posteriores suportadas.

- Configure o TLS nos Delivery Groups e nos VDAs depois de instalar componentes, criar um Site, criar catálogos de máquinas e criar Delivery Groups.
- Para configurar o TLS nos Delivery Groups, você deve ter permissão para alterar as regras de acesso do Controller. Um Administrador Completo tem essa permissão.
- Para configurar o TLS nos VDAs, você deve ser um administrador do Windows na máquina onde o VDA está instalado.
- Em VDAs agrupados que são provisionados por Machine Creation Services™ ou Provisioning Services, a imagem da máquina VDA é redefinida na reinicialização, fazendo com que as configurações TLS anteriores sejam perdidas. Execute o script PowerShell cada vez que o VDA for reiniciado para reconfigurar as configurações TLS.

**Aviso:**

Para tarefas que incluem trabalhar no registro do Windows — editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Para obter informações sobre como habilitar o TLS para o banco de dados do Site, consulte CTX137556.

## Instalar certificados de servidor TLS em Controladores

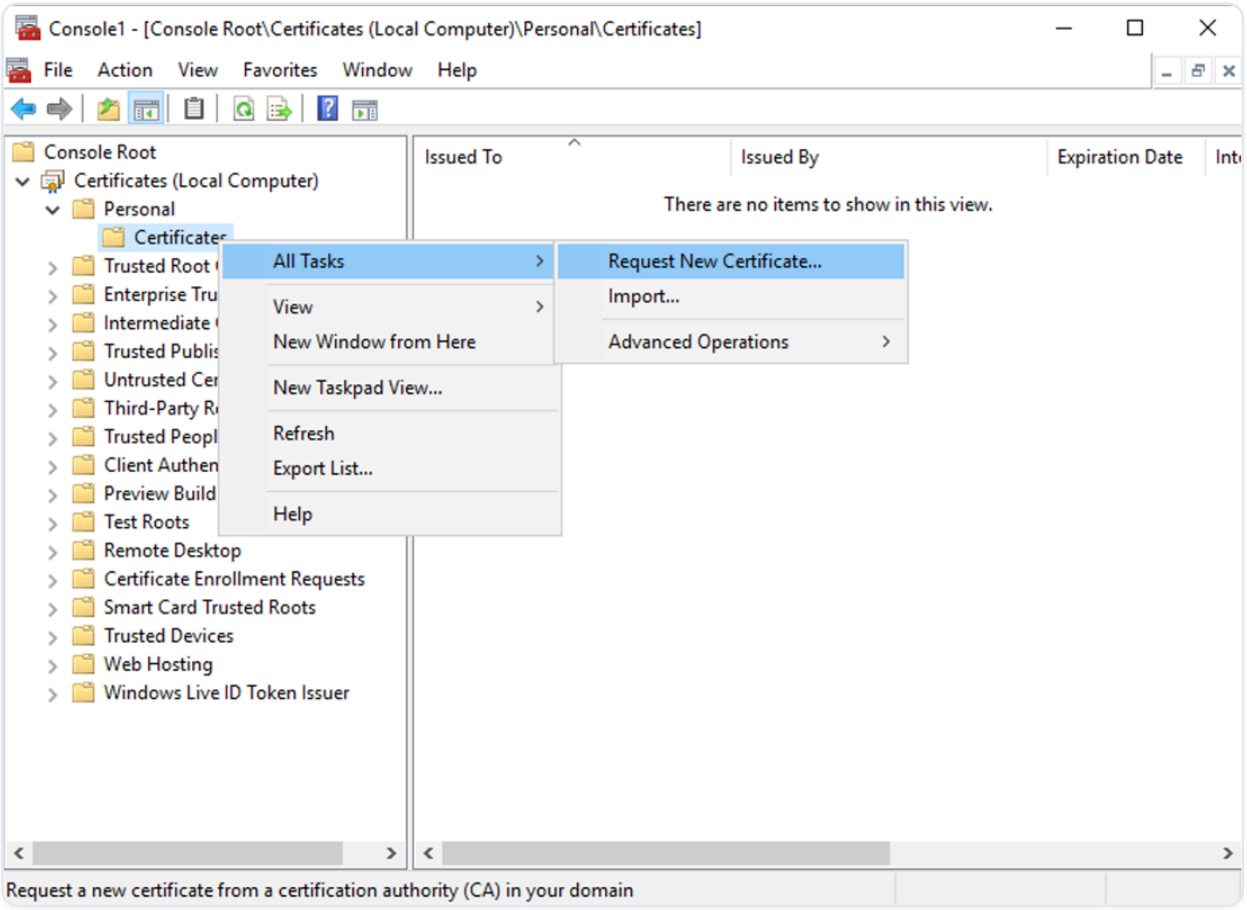
Para HTTPS, o Serviço XML oferece suporte a recursos TLS usando certificados de servidor, não certificados de cliente. Esta seção descreve a aquisição e instalação de certificados TLS em Delivery Controllers. As mesmas etapas podem ser aplicadas a Cloud Connectors para criptografar o tráfego STA e XML.

Embora existam vários tipos diferentes de autoridades de certificação e métodos para solicitar certificados delas, este artigo descreve a Autoridade de Certificação da Microsoft. A Autoridade de Certificação da Microsoft precisa ter um modelo de certificado publicado com a finalidade de Autenticação de Servidor.

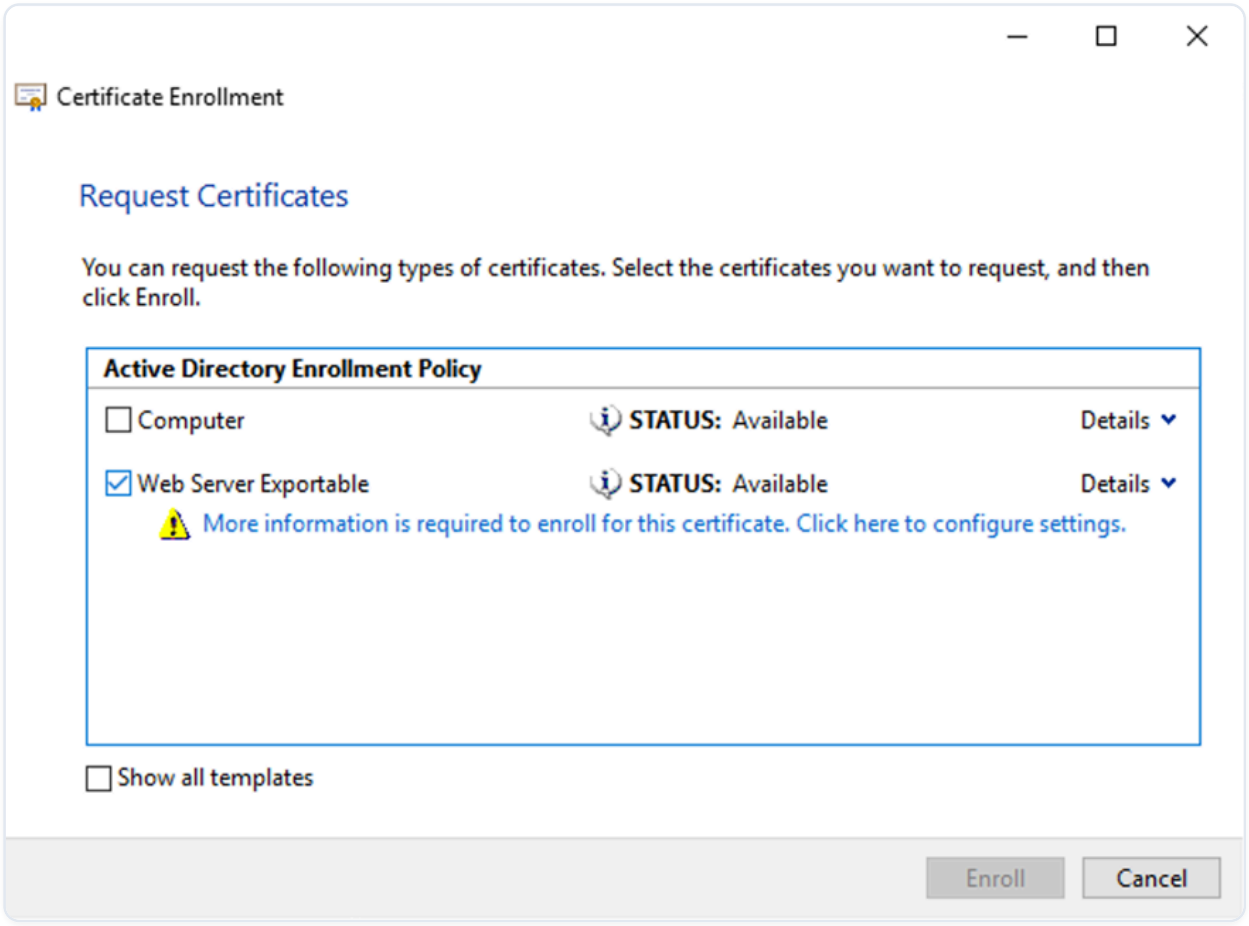
Se a Autoridade de Certificação da Microsoft estiver integrada a um domínio do Active Directory ou à floresta confiável à qual os Delivery Controllers estão unidos, você poderá adquirir um certificado do assistente de Registro de Certificado do snap-in Certificados do MMC.

### Solicitando e instalando um certificado

1. No Delivery Controller™, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando do menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.



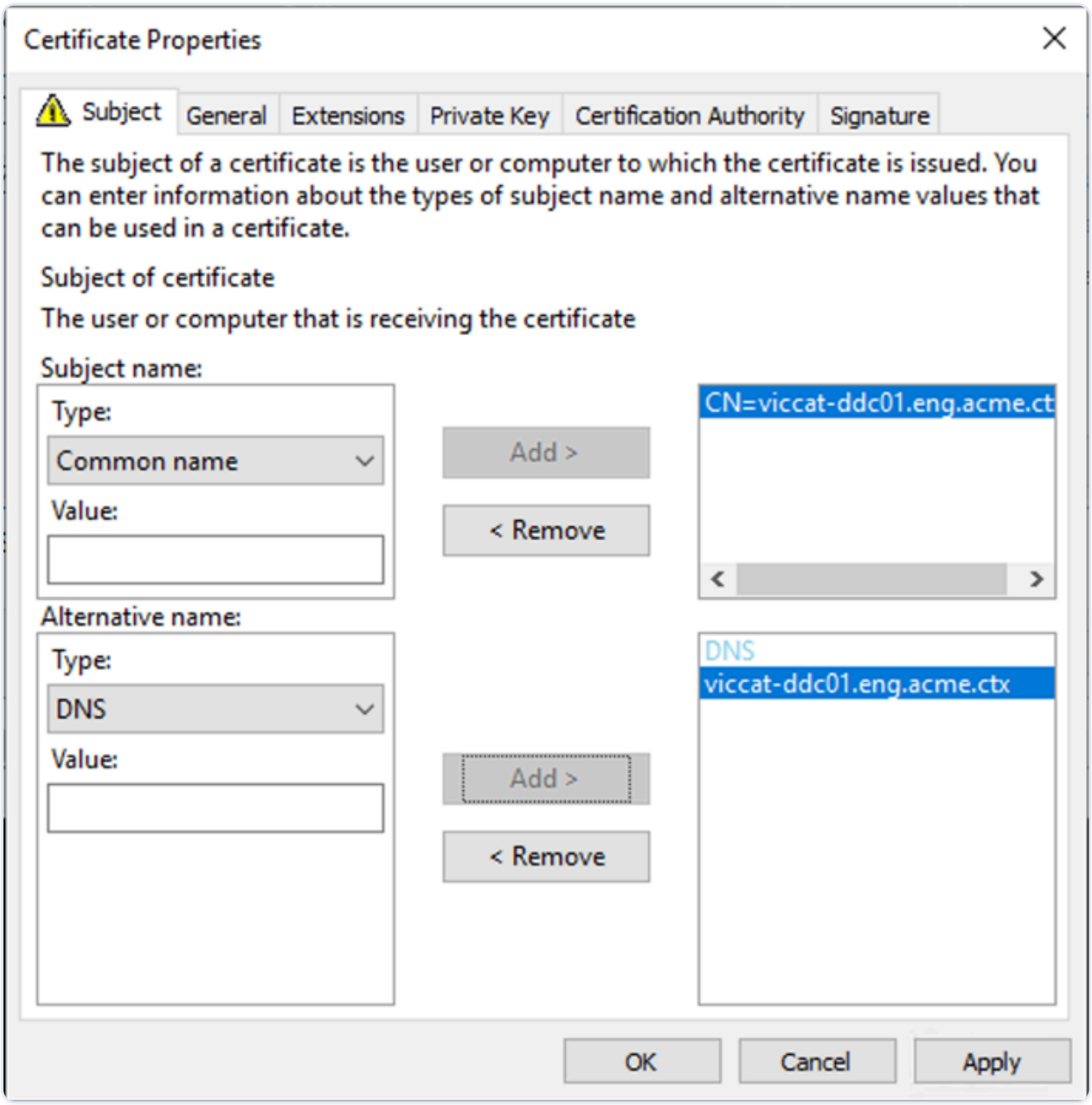

3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.
4. Selecione o modelo para o certificado de Autenticação de Servidor. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você poderá clicar em **Registrar** sem fornecer mais detalhes.




5. Para fornecer mais detalhes para o modelo de certificado, clique no botão de seta **Detalhes** e configure o seguinte:

   **Nome do assunto**: selecione Nome Comum e adicione o FQDN do Delivery Controller.

   **Nome alternativo**: selecione DNS e adicione o FQDN do Delivery Controller.




### Configurando a porta do listener SSL/TLS

1. Abra uma janela de comando do PowerShell como administrador da máquina.
2. Execute os seguintes comandos para obter o GUID do Aplicativo do Serviço de Broker:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root HKEY_CLASSES_ROOT



$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -Ea 0 |
Where-Object { $key = $_; $_.GetValueNames() | ForEach-Object
{ $key.GetValue($_) } | Where-Object { $_ -like 'Citrix Broker
Service' } } | Select-Object Name
```

```
$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)"
-ForegroundColor Yellow
```

3. Execute os seguintes comandos na mesma janela do PowerShell para obter o Thumbprint do certificado que você instalou anteriormente:

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

4. Execute os seguintes comandos na mesma janela do PowerShell para configurar a porta SSL/TLS do Serviço de Broker e usar o certificado para criptografia:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1  |
Select-Object -ExpandProperty IPV4Address



$IPPort = "$($IPV4_Address):443"



$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
appid={$Formatted_Guid}"



$SSLxml | netsh



. netsh http show sslcert
```

Quando configurado corretamente, a saída do último comando `.netsh http show sslcert` mostra que o listener está usando o `IP:port` correto e que `Application ID` corresponde ao GUID do Aplicativo do Serviço de Broker.

Desde que os servidores confiem no certificado instalado nos Delivery Controllers, agora você pode configurar os Delivery Controllers do StoreFront™ e as associações STA do Citrix Gateway para usar HTTPS em vez de HTTP.

**Nota:**

Se o Controller estiver instalado no Windows Server 2016 e o StoreFront estiver instalado no Windows Server 2012 R2, será necessária uma alteração de configuração no Controller para alterar a ordem das suites de cifras TLS. Essa alteração de configuração não é necessária para Controller e StoreFront com outras combinações de versões do Windows Server.

A lista de ordem de suites de cifras deve incluir as suites de cifras `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou

> `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (ou ambas); e essas suites de cifras devem preceder quaisquer suites de cifras `TLS_DHE_`.

1. Usando o Editor de Política de Grupo da Microsoft, navegue até **Configuração do Computador > Modelos Administrativos > Rede > Configurações de Configuração SSL**.
2. Edite a política "Ordem da Suite de Cifras SSL". Por padrão, esta política é definida como "Não Configurado". Defina esta política como Habilitado.
3. Organize as suites na ordem correta; remova quaisquer suites de cifras suites que você não deseja usar.

Certifique-se de que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` preceda quaisquer suites de cifras `TLS_DHE_`.

Na MSDN da Microsoft, consulte também Priorizando Suites de Cifras Schannel.

## Alterar portas HTTP ou HTTPS

Por padrão, o Serviço XML no Controller escuta na porta 80 para tráfego HTTP e na porta 443 para tráfego HTTPS. Embora você possa usar portas não padrão, esteja ciente dos riscos de segurança de expor um Controller a redes não confiáveis. A implantação de um servidor StoreFront autônomo é preferível a alterar os padrões.

Para alterar as portas HTTP ou HTTPS padrão usadas pelo Controller, execute o seguinte comando no Studio:

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

onde `<http-port>` é o número da porta para tráfego HTTP e `<https-port>` é o número da porta para tráfego HTTPS.

> **Nota:**

> Após alterar uma porta, o Studio pode exibir uma mensagem sobre compatibilidade de licença e atualização. Para resolver o problema, registre novamente as instâncias de serviço usando a seguinte sequência de cmdlets do PowerShell:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|
```

```
Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

### Impor apenas tráfego HTTPS

Se você quiser que o Serviço XML ignore o tráfego HTTP, crie a seguinte configuração de registro em HKLM\Software\Citrix\DesktopServer\ no Controller e, em seguida, reinicie o Serviço Broker.

Para ignorar o tráfego HTTP, crie o DWORD XmlServicesEnableNonSsl e defina-o como 0.

Existe um valor DWORD de registro correspondente que você pode criar para ignorar o tráfego HTTPS: DWORD XmlServicesEnableSsl. Certifique-se de que não esteja definido como 0.

## Configurações TLS em VDAs

Um Grupo de Entrega não pode ter uma mistura de alguns VDAs com TLS configurado e alguns VDAs sem TLS configurado. Antes de configurar o TLS para um Grupo de Entrega, certifique-se de que você já configurou o TLS para todos os VDAs nesse Grupo de Entrega.

Ao configurar o TLS em VDAs, as permissões no certificado TLS instalado são alteradas, concedendo ao Serviço ICA® acesso de leitura à chave privada do certificado e informando o Serviço ICA sobre o seguinte:

- **Qual certificado no armazenamento de certificados usar para TLS**.
- **Qual número de porta TCP usar para conexões TLS**.

  O Firewall do Windows (se ativado) deve ser configurado para permitir a conexão de entrada nesta porta TCP. Esta configuração é feita automaticamente para você ao usar o script PowerShell.
- **Quais versões do protocolo TLS permitir.**

> **Importante:**
>
> A Citrix recomenda que você revise o uso do SSLv3 e reconfigure essas implantações para remover o suporte ao SSLv3 quando apropriado. Consulte CTX200238.

> As versões de protocolo TLS suportadas seguem uma hierarquia (da mais baixa para a mais alta): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3. Especifique a versão mínima permitida; todas as conexões de protocolo usando essa versão ou uma versão superior são permitidas.

Por exemplo, se você especificar TLS 1.1 como a versão mínima, as conexões de protocolo TLS 1.1 e TLS 1.3 serão permitidas. Se você especificar SSL 3.0 como a versão mínima, as conexões para todas as versões suportadas serão permitidas. Se você especificar TLS 1.3 como a versão mínima, apenas as conexões TLS 1.3 serão permitidas.

DTLS 1.0 corresponde a TLS 1.1, e DTLS 1.3 corresponde a TLS 1.3.

- **Quais conjuntos de cifras TLS permitir.**

  Um conjunto de cifras seleciona a criptografia usada para uma conexão. Clientes e VDAs podem suportar diferentes conjuntos de cifras. Quando um cliente (aplicativo Citrix Workspace ou StoreFront) se conecta e envia uma lista de conjuntos de cifras TLS suportados, o VDA compara um dos conjuntos de cifras do cliente com um dos conjuntos de cifras em sua própria lista de conjuntos de cifras configurados e aceita a conexão. Se não houver um conjunto de cifras correspondente, o VDA rejeita a conexão.

  O VDA suporta três conjuntos de cifras (também conhecidos como modos de conformidade): GOV(erno), COM(ercial) e ALL. Os conjuntos de cifras aceitáveis também dependem do modo FIPS do Windows; consulte `<http://support.microsoft.com/kb/811833>` para obter informações sobre o modo FIPS do Windows. A tabela a seguir lista os conjuntos de cifras em cada conjunto:

| CONJUNTO DE CIFRAS TLS/ DTLS | TODOS | COM | GOV | TODOS | COM | GOV |
|---|---|---|---|---|---|---|
| **Modo FIPS** | Desativado | Desativado | Desativado | Ativado | Ativado | Ativado |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* | X | | X | X | | X |

| CONJUNTO DE CIFRAS TLS/ DTLS | TODOS | COM | GOV | TODOS | COM | GOV |
|---|---|---|---|---|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | X | | X | X | | X |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | X | X | | X | X | |

* Não suportado no Windows Server 2012 R2.

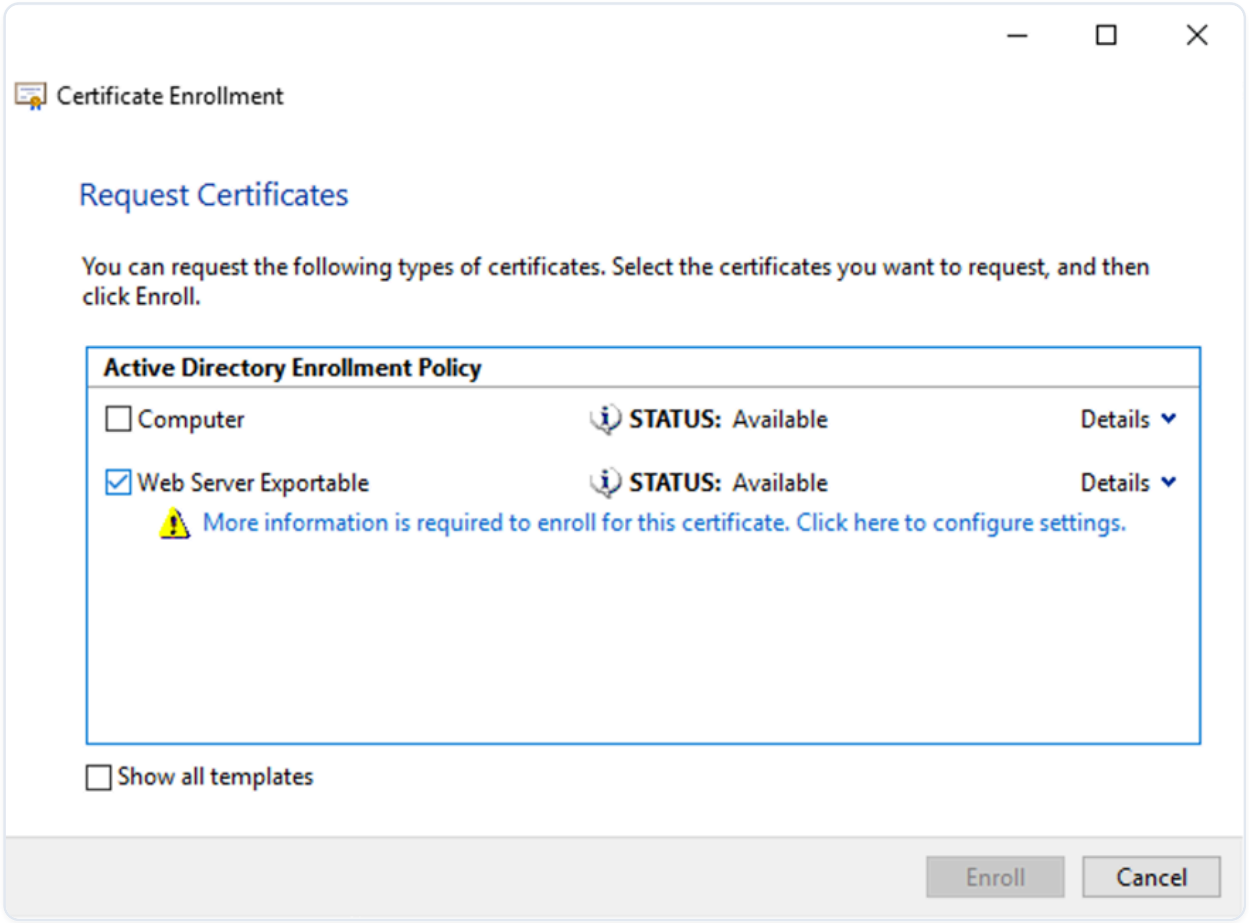
**Nota:**

O VDA não suporta conjuntos de cifras DHE (por exemplo, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 e TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Se selecionados pelo Windows, eles podem não ser usados pelo Receiver.

Se você estiver usando um Citrix Gateway, consulte a documentação do Citrix ADC para obter informações sobre o suporte a conjuntos de cifras para comunicação de back-end. Para obter informações sobre o suporte a conjuntos de cifras TLS, consulte Cifras disponíveis nos dispositivos Citrix ADC. Para obter informações sobre o suporte a conjuntos de cifras DTLS, consulte Suporte a cifras DTLS.

### Solicitando e instalando um certificado

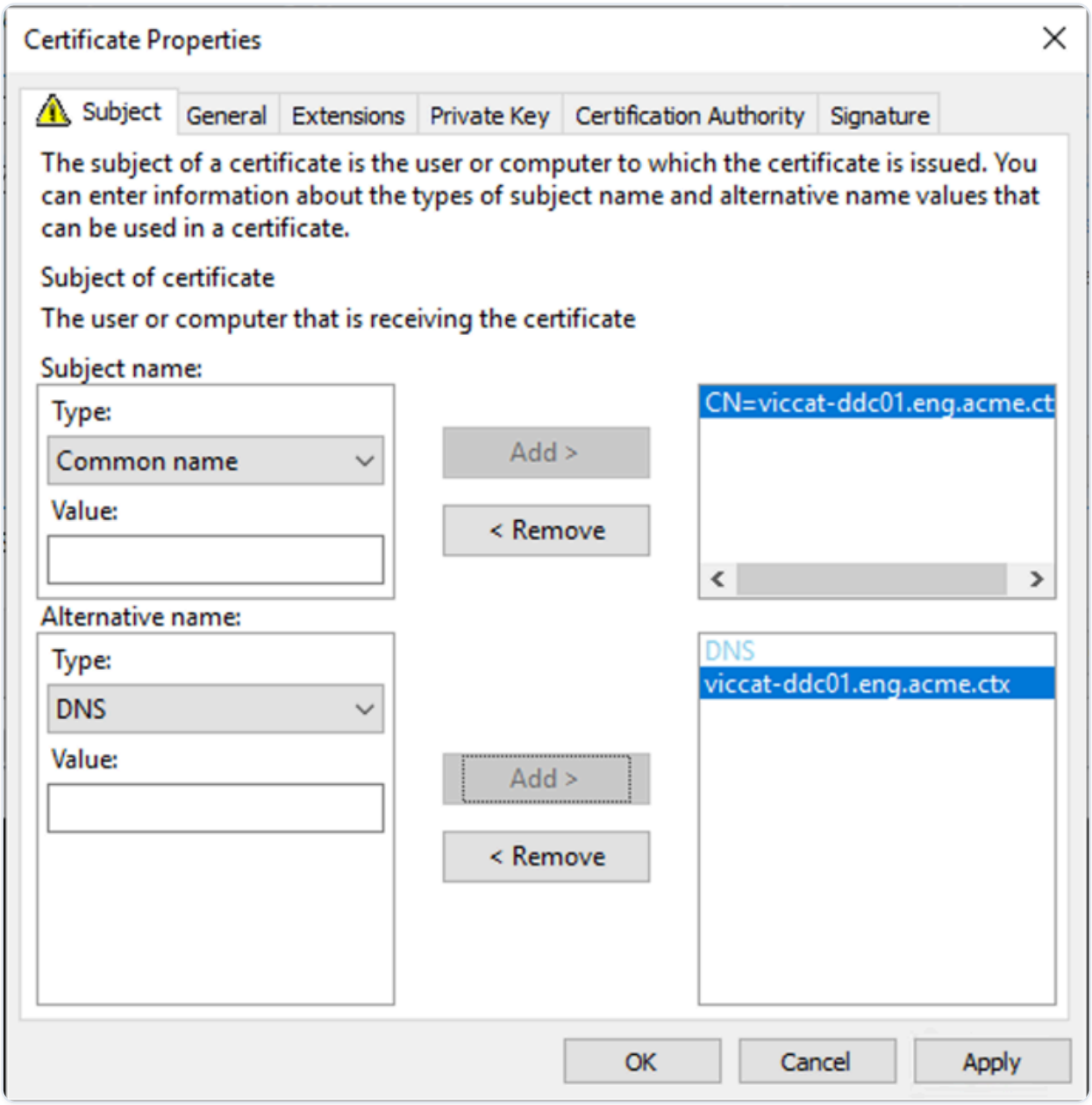
1. No VDA, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando do menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.
3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.
4. Selecione o modelo para o certificado de Autenticação de Servidor. Ambos os padrões do Windows, **Computador** ou **Servidor Web Exportável**, são aceitáveis. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você pode clicar em **Registrar** sem fornecer mais detalhes.




5. Para fornecer mais detalhes para o modelo de certificado, clique em **Detalhes** e configure o seguinte:

   **Nome do assunto** — selecione o tipo **Nome comum** e adicione o FQDN do VDA

   **Nome alternativo** — selecione o tipo **DNS** e adicione o FQDN do VDA



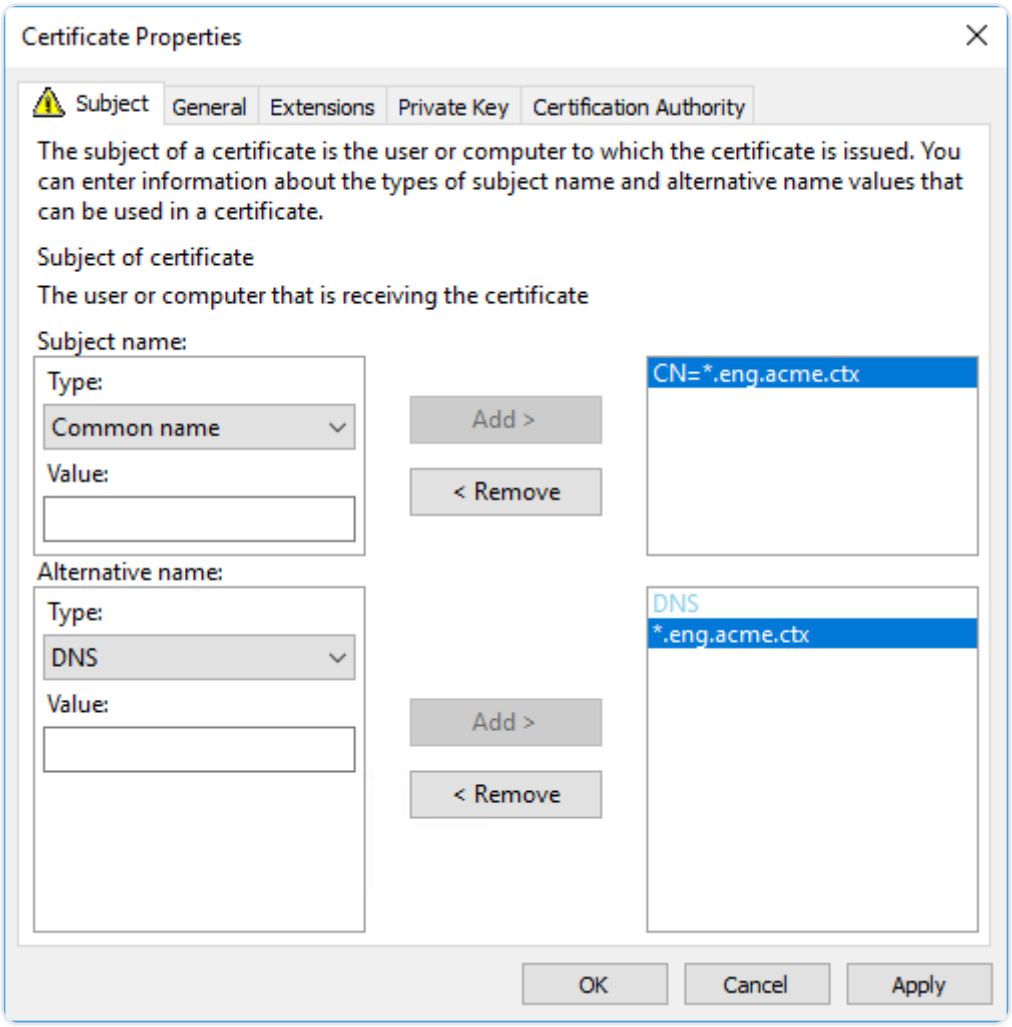

**Observação:**

Use o Registro Automático de Certificados dos Serviços de Certificados do Active Directory para automatizar a emissão e implantação de certificados nos VDAs. Isso é descrito em `<https://support.citrix.com/article/CTX205473>`.

Você pode usar certificados curinga para permitir que um único certificado proteja vários VDAs:

**Nome do assunto** — selecione o tipo **Nome comum** e insira o *.primary.domain dos VDAs

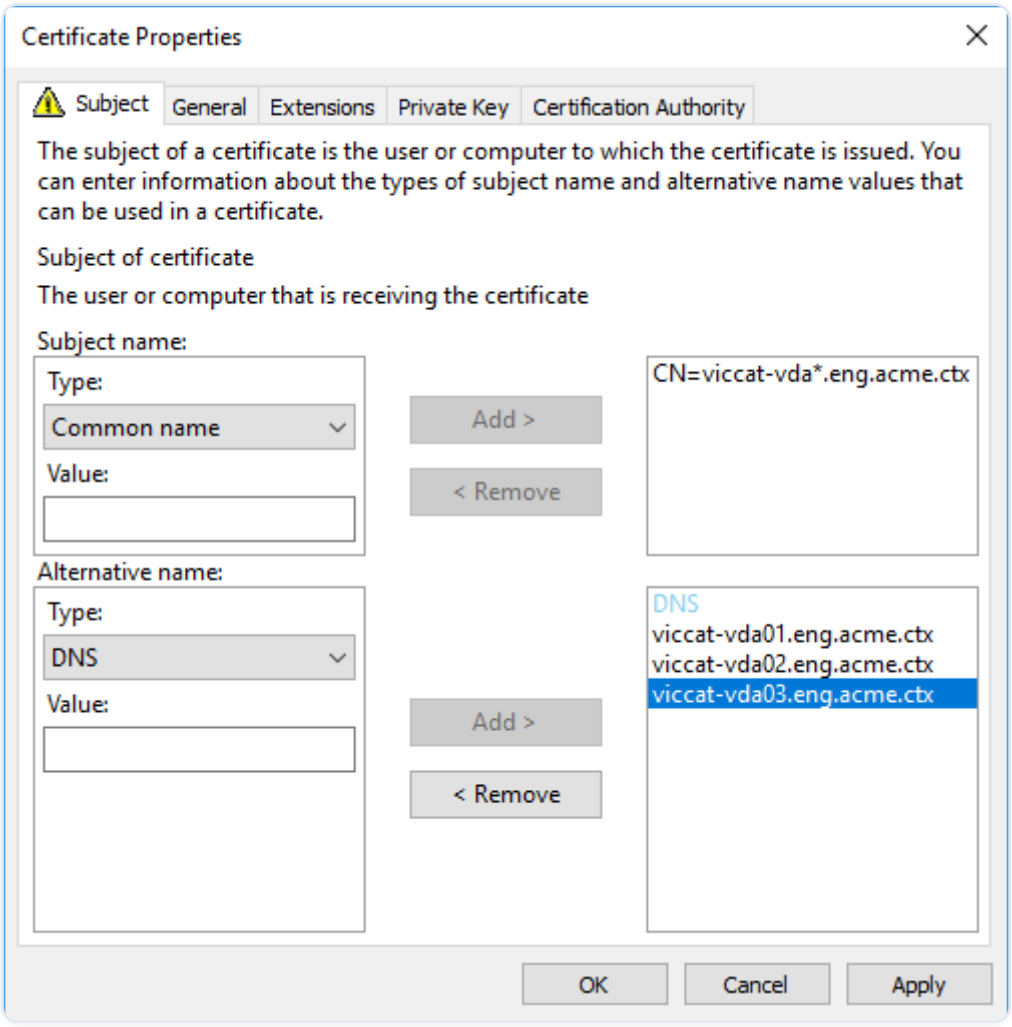
**Nome alternativo** — selecione o tipo **DNS** e adicione o *.primary.domain dos VDAs




Você pode usar certificados SAN para permitir que um único certificado proteja vários VDAs específicos:

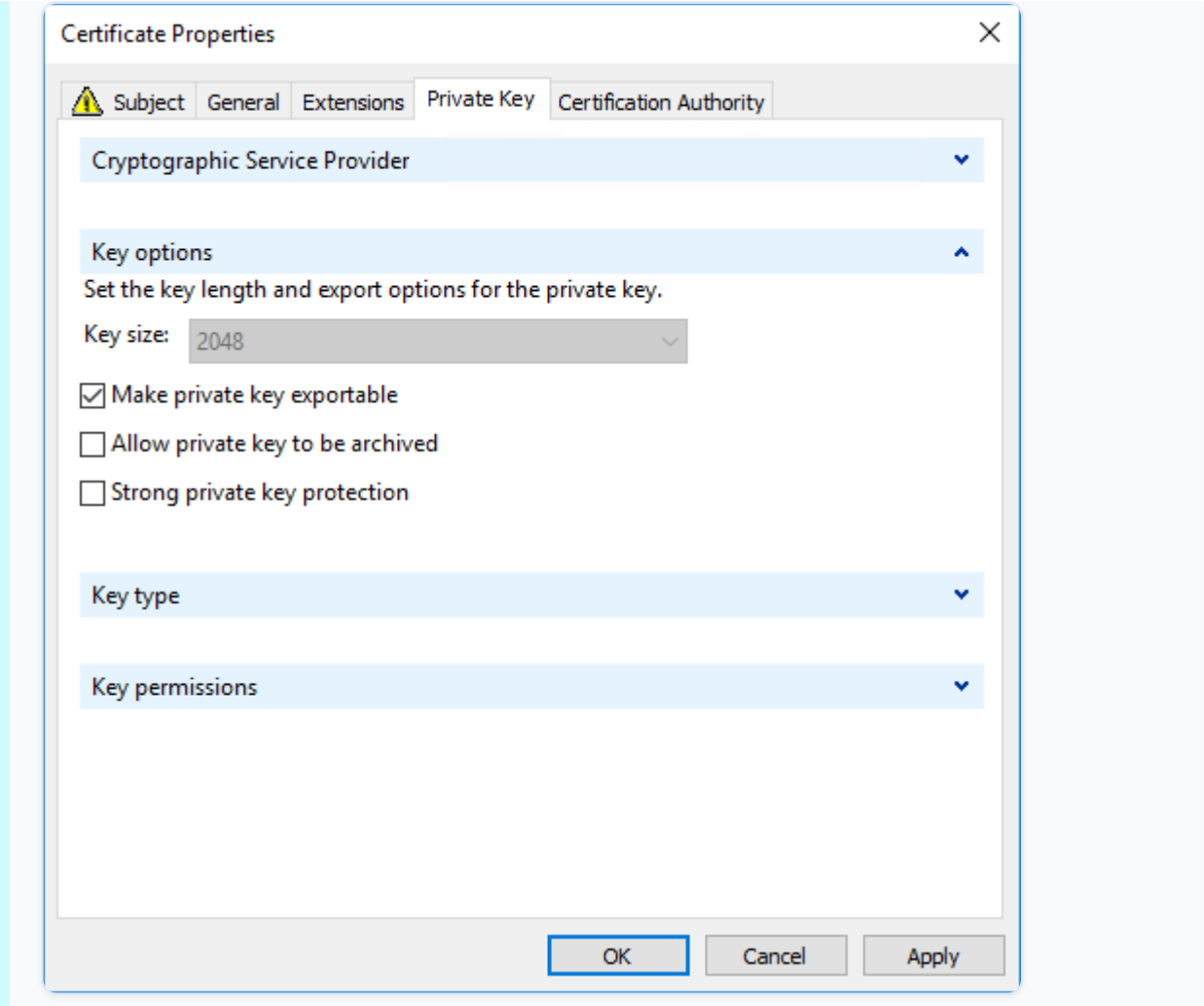
**Nome do assunto** — selecione o tipo **Nome comum** e insira uma string para ajudar a identificar o uso do certificado

**Nome alternativo** — selecione o tipo **DNS** e adicione uma entrada para o FQDN de cada VDA. Mantenha o número de Nomes alternativos no mínimo para garantir a negociação TLS ideal.




**Observação:**

Tanto certificados curinga quanto SAN exigem que **Tornar a chave privada exportável** na guia Chave Privada esteja selecionado:




### Configurar TLS em um VDA usando o script PowerShell

Instale o Certificado TLS na área Computador Local > Pessoal > Certificados do armazenamento de certificados. Se mais de um certificado residir nesse local, forneça o thumbprint do certificado para o script PowerShell.

> **Observação:**
>
> A partir do XenApp e XenDesktop 7.16 LTSR, o script PowerShell encontra o certificado correto com base no FQDN do VDA. Você não precisa fornecer o thumbprint quando apenas um único certificado está presente para o FQDN do VDA.

> O script Enable-VdaSSL.ps1 habilita ou desabilita o ouvinte TLS em um VDA. Este script está disponível na pasta *Support* > *Tools* > *SslSupport* na mídia de instalação.

Ao habilitar o TLS, os conjuntos de cifras DHE são desabilitados. Os conjuntos de cifras ECDHE não são afetados.

Ao habilitar o TLS, o script desabilita todas as regras existentes do Firewall do Windows para a porta TCP especificada. Em seguida, ele adiciona uma nova regra que permite que o Serviço ICA aceite conexões de entrada apenas nas portas TCP e UDP TLS. Ele também desabilita as regras do Firewall do Windows para:

- Citrix ICA (padrão: 1494)
- Citrix CGP (padrão: 2598)
- Citrix WebSocket (padrão: 8008)

O efeito é que os usuários só podem se conectar usando TLS ou DTLS. Eles não podem usar ICA/HDX, ICA/HDX com Confiabilidade da Sessão ou HDX sobre WebSocket, sem TLS ou DTLS.

> **Observação:**
>
> DTLS não é compatível com Áudio ICA/HDX sobre Transporte UDP em Tempo Real, ou com ICA/HDX Framehawk.
>
> Consulte Portas de rede.

O script contém as seguintes descrições de sintaxe, além de exemplos extras; você pode usar uma ferramenta como o Notepad++ para revisar essas informações.

> **Importante:**
>
> Especifique o parâmetro Enable ou Disable, e o parâmetro CertificateThumbPrint. Os outros parâmetros são opcionais.

**Sintaxe**

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

| PARÂMETRO | DESCRIÇÃO |
|---|---|
| Enable | Instala e habilita o ouvinte TLS no VDA. Este parâmetro ou o parâmetro Disable é obrigatório. |

| PARÂMETRO | DESCRIÇÃO |
| --- | --- |
| Disable | Desabilita o ouvinte TLS no VDA. Este parâmetro ou o parâmetro Enable é obrigatório. Se você especificar este parâmetro, nenhum outro parâmetro será válido. |
| ImpressãoDigitalDoCertificado "<impressão_digital>" | Impressão digital do certificado TLS no armazenamento de certificados, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar. Se este parâmetro for omitido, um certificado incorreto será selecionado. |
| PortaSSL <porta> | Porta TLS. Padrão: 443 |
| SSLMinVersion "<versão>" | Versão mínima do protocolo TLS, entre aspas. Valores válidos: “TLS_1.0” (padrão), “TLS_1.1” e “TLS_1.3”. |
| SSLCipherSuite "<suíte>" | Conjunto de cifras TLS, entre aspas. Valores válidos: "GOV", "COM" e "ALL" (padrão). |

### Exemplos

O script a seguir instala e habilita o valor da versão do protocolo TLS. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

O script a seguir instala e habilita o ouvinte TLS e especifica a porta TLS 400, o conjunto de cifras GOV e um valor mínimo de protocolo TLS 1.2. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.3"
```

```
-SSLCipherSuite "All"
```

O script a seguir desabilita o ouvinte TLS no VDA.

```
Enable-VdaSSL -Disable
```

### Configurar manualmente o TLS em um VDA

Ao configurar o TLS em um VDA manualmente, você concede acesso de leitura genérico à chave privada do certificado TLS para o serviço apropriado em cada VDA: NT SERVICE\PorticaService para um VDA para SO de sessão única do Windows, ou NT SERVICE\TermService para um VDA para SO de múltiplas sessões do Windows. Na máquina onde o VDA está instalado:

**ETAPA 1**. Inicie o console de gerenciamento da Microsoft (MMC): Iniciar > Executar > mmc.exe.

**ETAPA 2**. Adicione o snap-in Certificados ao MMC:

1. Selecione Arquivo > Adicionar/Remover Snap-in.
2. Selecione Certificados e clique em Adicionar.
3. Quando solicitado com "Este snap-in sempre gerenciará certificados para:", escolha "Conta de computador" e clique em Avançar.
4. Quando solicitado com "Selecione o computador que você deseja que este snap-in gerencie", escolha "Computador local" e clique em Concluir.

**ETAPA 3**. Em Certificados (Computador Local) > Pessoal > Certificados, clique com o botão direito do mouse no certificado e selecione Todas as Tarefas > Gerenciar Chaves Privadas.

**ETAPA 4.** O Editor da Lista de Controle de Acesso exibe "Permissões para chaves privadas (FriendlyName)" onde (FriendlyName) é o nome do seu certificado TLS. Adicione um dos seguintes serviços e conceda a ele acesso de Leitura:

- Para um VDA para SO de sessão única do Windows, "PORTICASERVICE"
- Para um VDA para Windows Multi-session OS, "TERMSERVICE"

**PASSO 5.** Clique duas vezes no certificado TLS instalado. Na caixa de diálogo do certificado, selecione a guia Detalhes e role até o final. Clique em Impressão digital.

**PASSO 6.** Execute regedit e vá para HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Edite a chave SSL Thumbprint e copie o valor da impressão digital do certificado TLS para este valor binário. Você pode ignorar com segurança itens desconhecidos na caixa de diálogo Editar Valor Binário (como '0000' e caracteres especiais).
2. Edite a chave SSLEnabled e altere o valor DWORD para 1. (Para desabilitar o SSL posteriormente, altere o valor DWORD para 0.)
3. Se você quiser alterar as configurações padrão (opcional), use o seguinte no mesmo caminho do registro:

   SSLPort DWORD – Número da porta SSL. Padrão: 443.

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.3. Padrão: 2 (TLS 1.0).

   SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Padrão: 3 (ALL).

**PASSO 7.** Certifique-se de que as portas TCP e UDP TLS estejam abertas no Firewall do Windows, caso não sejam a porta padrão 443. (Ao criar a regra de entrada no Firewall do Windows, certifique-se de que suas propriedades tenham as entradas "Permitir a conexão" e "Ativado" selecionadas.)

**PASSO 8.** Certifique-se de que nenhum outro aplicativo ou serviço (como o IIS) esteja usando a porta TCP TLS.

**PASSO 9.** Para VDAs para Windows Multi-session OS, reinicie a máquina para que as alterações entrem em vigor. (Você não precisa reiniciar máquinas que contêm VDAs para Windows Single-session OS.)

> **Importante:**

> Uma etapa extra é necessária quando o VDA está no Windows Server 2012 R2, Windows Server 2016 ou Windows 10 Anniversary Edition ou versão posterior suportada. Isso afeta as conexões do Citrix Receiver para Windows (versão 4.6 a 4.9), Citrix Workspace app para HTML5 e Citrix Workspace app para Chrome. Isso também inclui conexões usando o Citrix Gateway.

> Esta etapa também é necessária para todas as conexões que usam o Citrix Gateway, para todas as versões de VDA, se o TLS entre o Citrix Gateway e o VDA estiver configurado. Isso afeta todas as versões do Citrix Receiver™.

No VDA (Windows Server 2012 R2, Windows Server 2016 ou Windows 10 Anniversary Edition ou posterior), usando o Editor de Política de Grupo, vá para Configuração do Computador > Políticas > Modelos Administrativos > Rede > Configurações de Configuração SSL > Ordem do Conjunto de Cifras SSL. Selecione a seguinte ordem:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

**Nota:**

Os primeiros seis itens também especificam a curva elíptica, P384 ou P256. Certifique-se de que "curve25519" não esteja selecionado. O Modo FIPS não impede o uso de "curve25519".

Quando esta configuração de Política de Grupo é configurada, o VDA seleciona um conjunto de cifras somente se ele aparecer em ambas as listas: a lista da Política de Grupo e a lista para o modo de conformidade selecionado (COM, GOV ou ALL). O conjunto de cifras também deve aparecer na lista enviada pelo cliente (aplicativo Citrix Workspace ou StoreFront).

Esta configuração de Política de Grupo também afeta outros aplicativos e serviços TLS no VDA. Se seus aplicativos exigirem conjuntos de cifras específicos, pode ser necessário adicioná-los a esta lista de Política de Grupo.

**Importante:**

Embora as alterações da Política de Grupo sejam exibidas quando aplicadas, as alterações da Política de Grupo para a configuração TLS só entram em vigor após a reinicialização do

> sistema operacional. Portanto, para desktops agrupados, aplique as alterações da Política de Grupo para a configuração TLS à imagem base.

### Configurar TLS em Grupos de Entrega

Conclua este procedimento para cada Grupo de Entrega que contém VDAs que você configurou para conexões TLS.

1. No Studio, abra o console do PowerShell.
2. Execute **asnp Citrix.*** para carregar os cmdlets do produto Citrix.
3. Execute **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Execute **Set-BrokerSite -DnsResolutionEnabled $true**.

### Solução de problemas

Se ocorrer um erro de conexão, verifique o log de eventos do sistema no VDA.

Ao usar o aplicativo Citrix Workspace para Windows, se você receber um erro de conexão que indica um erro TLS, desative o Desktop Viewer e tente conectar novamente. Embora a conexão ainda falhe, uma explicação do problema TLS subjacente pode ser fornecida. Por exemplo, você especificou um modelo incorreto ao solicitar um certificado da autoridade de certificação.)

A maioria das configurações que usam o HDX™ Adaptive Transport funciona com sucesso com DTLS, incluindo aquelas que usam as versões mais recentes do aplicativo Citrix Workspace, Citrix Gateway e o VDA. Algumas configurações que usam DTLS entre o aplicativo Citrix Workspace e o Citrix Gateway, e que usam DTLS entre o Citrix Gateway e o VDA, exigem ação adicional.

Ação adicional é necessária se:

- a versão do Citrix Receiver suporta HDX Adaptive Transport e DTLS: Receiver para Windows (4.7, 4.8, 4.9), Receiver para Mac (12.5, 12.6, 12.7), Receiver para iOS (7.2, 7.3.x) ou Receiver para Linux (13.7)

e uma das seguintes opções também se aplica:

- a versão do Citrix Gateway oferece suporte a DTLS para o VDA, mas a versão do VDA não oferece suporte a DTLS (versão 7.15 ou anterior),
- a versão do VDA oferece suporte a DTLS (versão 7.16 ou posterior), mas a versão do Citrix Gateway não oferece suporte a DTLS para o VDA.

Para evitar que as conexões do Citrix Receiver falhem, faça uma das seguintes ações:

- atualize o Citrix Receiver para a versão 4.10 ou posterior do Receiver para Windows, 12.8 ou posterior do Receiver para Mac, ou 7.5 ou posterior do Receiver para iOS; ou,
- atualize o Citrix Gateway para uma versão que ofereça suporte a DTLS para o VDA; ou,
- atualize o VDA para a versão 7.16 ou posterior; ou,
- desative o DTLS no VDA; ou,
- desative o HDX Adaptive Transport.

**Nota:**

Uma atualização adequada para o Receiver para Linux ainda não está disponível. O Receiver para Android (versão 3.12.3) não oferece suporte a HDX Adaptive Transport e DTLS via Citrix Gateway e, portanto, não é afetado.

Para desativar o DTLS no VDA, modifique a configuração do firewall do VDA para desativar a porta UDP 443. Consulte Portas de rede.

## Comunicação entre Controller e VDA

A proteção em nível de mensagem do Windows Communication Framework (WCF) protege a comunicação entre o Controller e o VDA. Não é necessária proteção extra em nível de transporte usando TLS. A configuração do WCF usa Kerberos para autenticação mútua entre o Controller e o VDA. A criptografia usa AES no modo CBC com uma chave de 256 bits. A integridade da mensagem usa SHA-1.

De acordo com a Microsoft, os protocolos de segurança usados pelo WCF estão em conformidade com os padrões da OASIS (Organization for the Advancement of Structured Information Standards), incluindo o WS-SecurityPolicy 1.2. Além disso, a Microsoft afirma que o WCF oferece suporte a todos os conjuntos de algoritmos listados em Security Policy 1.2.

A comunicação entre o Controller e o VDA usa o conjunto de algoritmos basic256, cujos algoritmos são os mencionados acima.

### TLS e redirecionamento de vídeo HTML5, e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX em execução no VDA. Para conseguir isso, o Serviço de Redirecionamento de Vídeo HTML5 gera dois certificados personalizados no armazenamento de certificados no VDA. A interrupção do serviço remove os certificados.

A política de redirecionamento de vídeo HTML5 está desabilitada por padrão.

O redirecionamento de conteúdo do navegador está habilitado por padrão.

Para obter mais informações sobre o redirecionamento de vídeo HTML5, consulte Configurações de política de multimídia.

## Habilitar TLS em Delivery Controllers

Por padrão, tanto HTTP quanto HTTPS estão habilitados. HTTPS usa um certificado autoassinado com o FQDN do servidor como nome comum, que não é confiável pelo StoreFront™ ou navegadores da web.

Para habilitar o TLS em um delivery controller™, você deve:

- Obter, instalar e registrar um certificado de servidor em todos os Delivery Controllers. Para detalhes, consulte Solicitando e instalando um certificado.
- Configurar uma porta com o certificado TLS. Para detalhes, consulte Instalando um certificado.
- Habilitar HTTPS para o serviço de monitoramento.
- Impor tráfego HTTPS desabilitando HTTP. Para mais detalhes, consulte Impor tráfego HTTPS apenasImpor tráfego HTTPS apenas.
- Opcionalmente, você pode alterar as portas que o Controller usa para escutar o tráfego HTTP e HTTPS. Para mais detalhes, consulte Alterar portas HTTP ou HTTPS.

### Solicitando e instalando um certificado

Para usar TLS, você deve instalar um certificado cujo Nome Comum ou Nome Alternativo do Assunto corresponda ao FQDN do servidor. Se você estiver usando um balanceador de carga na frente dos delivery controllers, inclua os FQDNs do servidor e do balanceador de carga como Nomes Alternativos do Assunto. Para mais informações, consulte Certificados. Para que o

StoreFront se conecte ao delivery controller, você deve usar um algoritmo de assinatura digital RSA. O StoreFront não oferece suporte a certificados que usam o algoritmo ECDSA.

### Configurando a porta de escuta SSL/TLS

Se o componente IIS do Windows estiver instalado no mesmo servidor, que é instalado como parte do Web Studio e do Director, você pode configurar o TLS usando o IIS. Para mais informações, consulte Habilitar TLS no Web Studio e Director. Caso contrário, para configurar o certificado usando o PowerShell:

1. Para verificar se há um certificado existente vinculado, abra um prompt de comando e execute `netsh http show sslcert`:

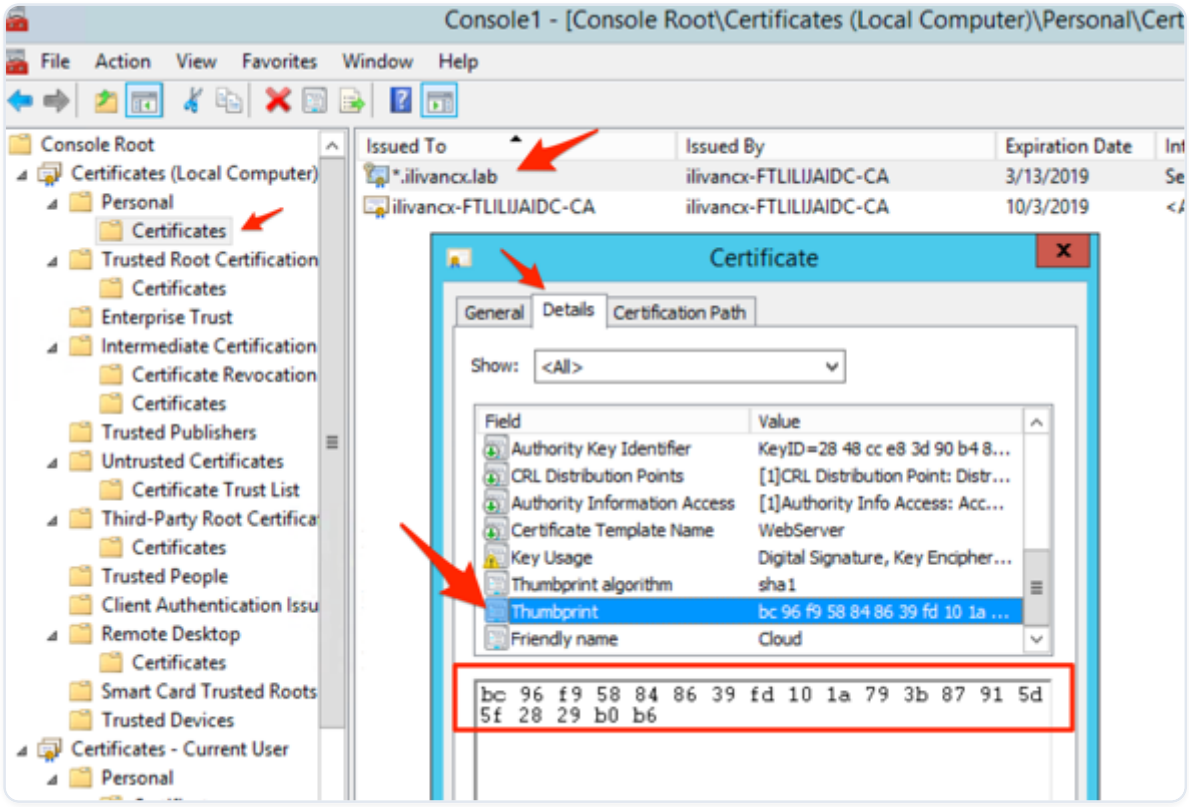
   ```
   netsh http show sslcert
   ```

2. Se houver uma vinculação existente, exclua-a.

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   Substituindo `0.0.0.0:443` por um endereço IP e porta específicos, se houver um especificado na vinculação existente.

3. Encontre a impressão digital do certificado que você instalou anteriormente. Para visualizar a impressão digital, abra **Gerenciar certificados do computador**, navegue até o certificado, abra-o e vá para a guia **Detalhes**.




Alternativamente, você pode usar o PowerShell. Por exemplo, o script a seguir procura um certificado cujo nome comum corresponde ao nome do host do servidor e imprime o thumbprint:

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

Se o nome comum do certificado não corresponder aos nomes de host, isso falhará. Se houver vários certificados para o nome do host, isso retornará vários thumbprints concatenados e você deverá escolher o thumbprint apropriado.

O exemplo a seguir procura um certificado por nome amigável:

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'
```

```
Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

Se houver vários certificados com o nome amigável especificado, isso retornará vários thumbprints concatenados e você deverá escolher o thumbprint apropriado.

4. Para vincular o certificado à porta, use o comando `netsh http add sslcert`:

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: O endereço IP e a porta. Usar 0.0.0.0:443 aplica isso a todos os endereços IP. Você pode, em vez disso, especificar um endereço IP específico.
- `certhash`: A impressão digital do certificado que você identificou na etapa anterior.
- `appid`: O GUID do Serviço de Broker da Citrix.

> **Nota:**
>
> Ao renovar um certificado ou refazer a vinculação, use o `appid` específico associado ao Serviço de Broker em vez de um GUID arbitrário.
>
> Para encontrar o `appid` correto para o Serviço de Broker da Citrix:

a. Abra uma janela de comando do PowerShell como administrador e execute o seguinte comando:

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. Localize o IdentifyingNumber (GUID) para o Serviço de Broker da Citrix na saída (por exemplo, `{D333C884-187F-447C-8C67-463F33989C8F}`). Use este GUID para o parâmetro `appid`.

- `disablelegacytls=enable`: Desabilita versões legadas do TLS. Este parâmetro está disponível no Windows 2022 e superior. No Windows 2022, ele desabilita o TLS 1.0 e 1.1. No Windows 2025, isso é desnecessário, pois o TLS 1.0 e 1.1 são desabilitados por padrão.

Por exemplo, execute o seguinte comando para vincular o certificado com a impressão digital `bc96f958848639fd101a793b87915d5f2829b0b6` à porta `443` em todos os endereços IP:

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

Uma vez que o HTTPS esteja habilitado, você deve configurar quaisquer implantações do StoreFront e Netscaler Gateways para usar HTTPS em vez de HTTP para se conectar ao controlador de entrega.

### Configurar a API OData do Serviço de Monitoramento para HTTPS

O serviço de monitoramento fornece APIs OData v3 e v4 para permitir que aplicativos Citrix® e de terceiros consultem dados. O Director se conecta ao serviço de monitoramento usando a API OData V3. Para configurar as APIs OData do monitor para HTTPS, conclua as seguintes etapas:

1. Execute o seguinte PowerShell:

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. Abra o arquivo `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` com um editor de texto. Encontre o elemento `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` e altere-o para `<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />`.

### Configurar conjuntos de cifras

A lista de ordem de conjuntos de cifras deve incluir os conjuntos de cifras `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (ou ambos); e esses conjuntos de cifras devem preceder quaisquer conjuntos de cifras `TLS_DHE_`.

1. Usando o Editor de Política de Grupo da Microsoft, navegue até **Configuração do Computador > Modelos Administrativos > Rede > Configurações de Configuração SSL**.
2. Edite a política "Ordem do Conjunto de Cifras SSL". Por padrão, esta política é definida como "Não Configurado". Defina esta política como Habilitada.
3. Organize os conjuntos na ordem correta; remova quaisquer conjuntos de cifras que você não deseja usar.

Certifique-se de que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` preceda quaisquer conjuntos de cifras `TLS_DHE_`.

No Microsoft Learn, consulte também Configurando a Ordem do Conjunto de Cifras TLS.

### Impor apenas tráfego HTTPS

Recomenda-se que você configure o Serviço XML para ignorar o tráfego HTTP.

1. Execute `regedit`
2. Abrir `HKLM\Software\Citrix\DesktopServer\`
3. Crie um novo valor DWORD com o nome `XmlServicesEnableNonSsl` e defina-o como 0.
4. Reinicie o Serviço Broker.

Existe um valor DWORD de registro correspondente `XmlServicesEnableSsl` que você pode criar para ignorar o tráfego HTTPS. Certifique-se de que não esteja definido como 0.

### Alterar portas HTTP ou HTTPS

Por padrão, o Serviço XML no Controller escuta na porta 80 para tráfego HTTP e na porta 443 para tráfego HTTPS. Embora você possa usar portas não padrão, esteja ciente dos riscos de segurança de expor um Controller a redes não confiáveis. A implantação de um servidor StoreFront autônomo é preferível a alterar os padrões.

Para alterar as portas HTTP ou HTTPS padrão usadas pelo Controller, execute o seguinte comando no Studio:

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

onde `<http-port>` é o número da porta para tráfego HTTP e `<https-port>` é o número da porta para tráfego HTTPS.

**Nota:**

Após alterar uma porta, o Studio pode exibir uma mensagem sobre compatibilidade de licença e atualização. Para resolver o problema, registre novamente as instâncias de serviço usando a seguinte sequência de cmdlets do PowerShell:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

## Habilitar TLS no Web Studio e Director

Recomendamos sempre usar TLS para proteger as conexões com o Web Studio e o Director, habilitando HTTPS. Este artigo explica como configurar o Web Studio e o Director para usar um certificado confiável e garantir acesso seguro via HTTPS.

### Comportamento padrão

Ao instalar o Web Studio, o instalador cria um certificado autoassinado e o vincula à porta 443 no servidor atual. Você pode acessar o Web Studio e o Director de um navegador da web via HTTPS no servidor local.

No entanto, se você tentar acessar o Web Studio ou o Director de outra máquina via HTTPS, o navegador exibirá um erro de segurança porque ele não confia no certificado.

**Nota:**

> Se você instalar o Director sem o Web Studio, o instalador não cria um certificado autoassinado.

### Habilitar acesso seguro via HTTPS

Para permitir o acesso ao Web Studio ou Director via HTTPS de máquinas que não sejam o servidor do Web Studio, siga estas etapas:

1. Criar ou importar um certificado confiável.
2. Vincular o certificado à porta 443 no IIS.
3. (Opcional) Habilitar HTTP Strict Transport Security (HSTS).
4. Se o Web Studio não estiver configurado como um proxy (as máquinas cliente se conectam tanto ao Web Studio quanto aos Delivery Controllers), habilitar TLS nos Delivery Controllers.

> **Nota:**
>
> Não é recomendado usar o certificado autoassinado porque ele exige configuração manual em cada máquina. Para obter mais informações, consulte Usar o certificado autoassinado.

### Criar ou importar um certificado confiável

Recomendamos usar um certificado de uma autoridade de certificação empresarial ou pública que seja confiável para as máquinas que se conectam ao servidor.

Para mais informações, consulte Criar um novo certificado e Importar certificado existente. O nome comum do certificado ou o nome alternativo do assunto deve corresponder ao FQDN que os usuários usam para se conectar ao Web Studio ou Director. Se um balanceador de carga for implantado na frente do servidor, use o FQDN do balanceador de carga.

### Vincular o certificado à porta 443

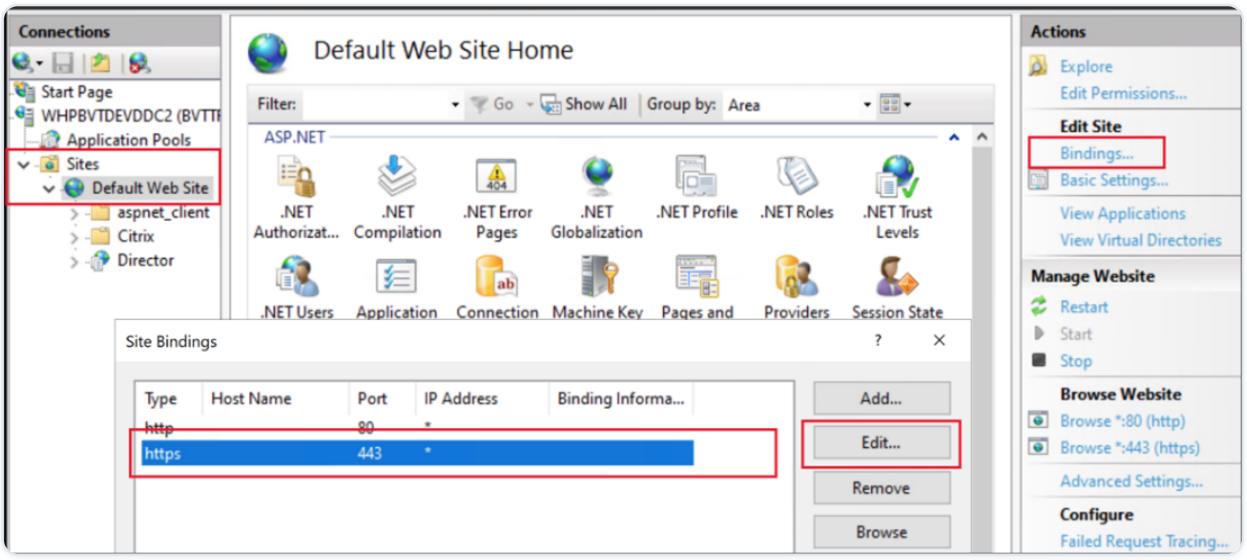
Após criar ou importar um certificado confiável, vincule-o à porta `443` no IIS. Você pode fazer isso antes ou depois da instalação. Se a vinculação do certificado já estiver configurada para a porta `443`, o instalador não fará alterações.

> **Nota:**

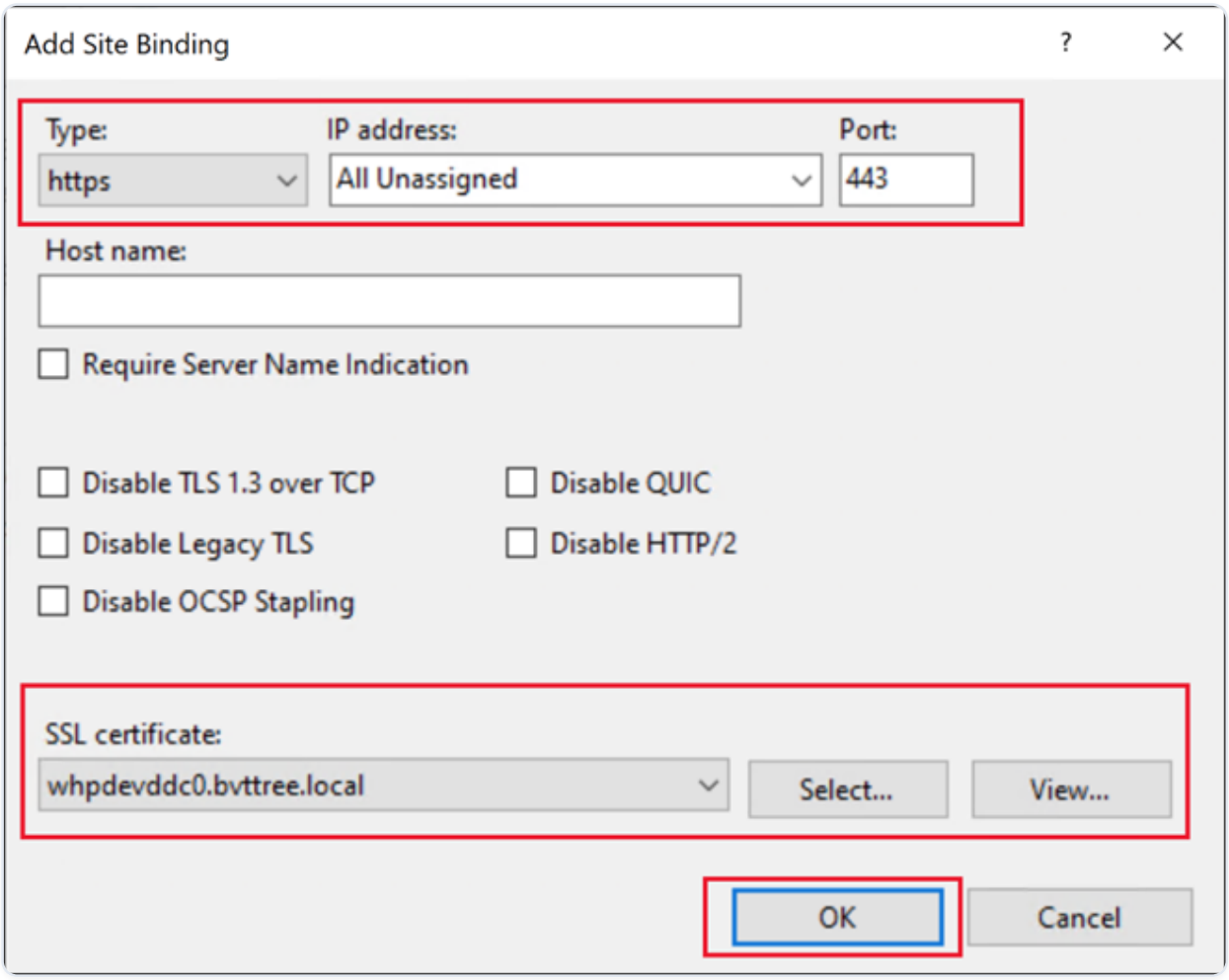
> Por padrão, o Web Studio e o Director usam a porta 443 para acesso HTTPS seguro. Você pode alterar o número da porta, se necessário. Consulte Alterar o número da porta padrão para obter detalhes.

> Para vincular o certificado à porta `443`, siga estas etapas:

1. Faça logon no servidor como administrador.
2. Abra o Gerenciador do IIS e navegue até **Sites > Default Web Site > Bindings**.
3. Se houver uma vinculação existente do tipo **https**, selecione-a e clique em **Editar...**. Se não houver vinculação **https**, clique em **Adicionar**.




4. Crie ou edite a vinculação do site:
   a. Para uma nova vinculação, defina o tipo como **https** e a porta como `443`.
   b. Selecione o certificado SSL apropriado.
   c. No Windows Server 2022 ou superior, opcionalmente selecione **Disable Legacy TLS** para garantir que os usuários possam se conectar apenas usando versões modernas de TLS.
   d. Clique em **OK**.




Alternativamente, você pode alterar o certificado usando o PowerShell. Por exemplo, o script a seguir procura um certificado com um nome comum fornecido e o vincula a todos os endereços IP, porta 443, e desabilita as versões legadas de TLS.

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

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

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

Observe que `appid` é um GUID arbitrário que pode ser usado para identificar qual aplicativo adicionou o certificado.

### Usar o certificado autoassinado

Você pode usar o certificado autoassinado existente, mas não é recomendado porque exige a configuração manual de cada máquina que acessa o servidor.

Para instalar o certificado autoassinado em máquinas que precisam se conectar ao Web Studio:

1. Exporte o certificado autoassinado existente dos servidores Web Studio e Delivery Controller.
2. Importe o certificado para o armazenamento de **Certificados Raiz Confiáveis** das máquinas que devem acessar o servidor.

### (Opcional) Habilitar HTTP Strict Transport Security (HSTS)

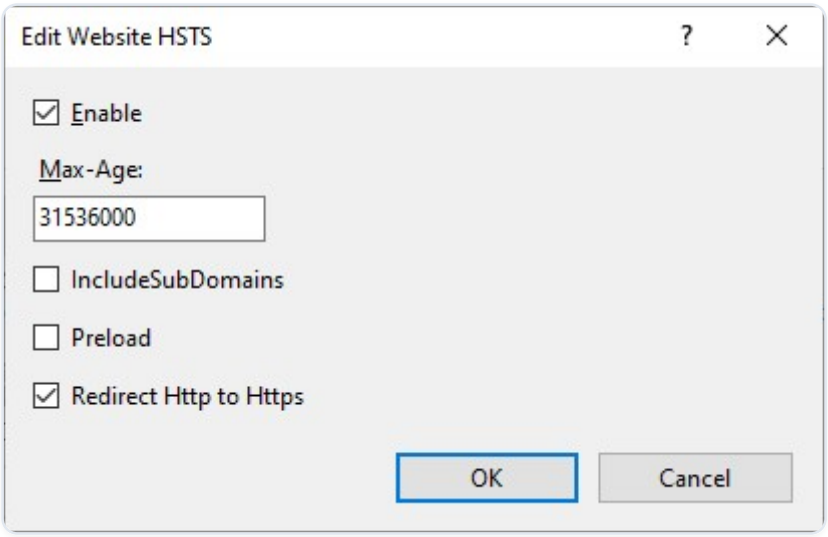
HTTP Strict Transport Security (HSTS) instrui os navegadores da web a usar apenas HTTPS ao acessar o site. Se um usuário tentar acessar a URL usando HTTP, o navegador alternará automaticamente para HTTPS. Essa configuração garante a validação de conexão segura nos lados do cliente e do servidor. O navegador mantém essa validação pelo período configurado.

No Windows Server 2019 e posterior, você pode configurar o HSTS no IIS:

1. Abra o **Gerenciador de Serviços de Informações da Internet (IIS)**.
2. Selecione **Site Padrão** (ou o site apropriado).
3. No painel **Ações** no lado direito, selecione **HSTS...**.
4. Selecione **Habilitar** e insira uma idade máxima, por exemplo, 31536000 para um ano.
5. Selecione **Redirecionar Http para Https**.

> **Observação:**
>
> O Web Studio configura automaticamente uma regra de **Reescrita de URL** para redirecionar HTTP para HTTPS ao acessar o site do Studio. No entanto, essa opção também se aplica ao Director e a quaisquer outros aplicativos no site do IIS.

6. Clique em **OK**.

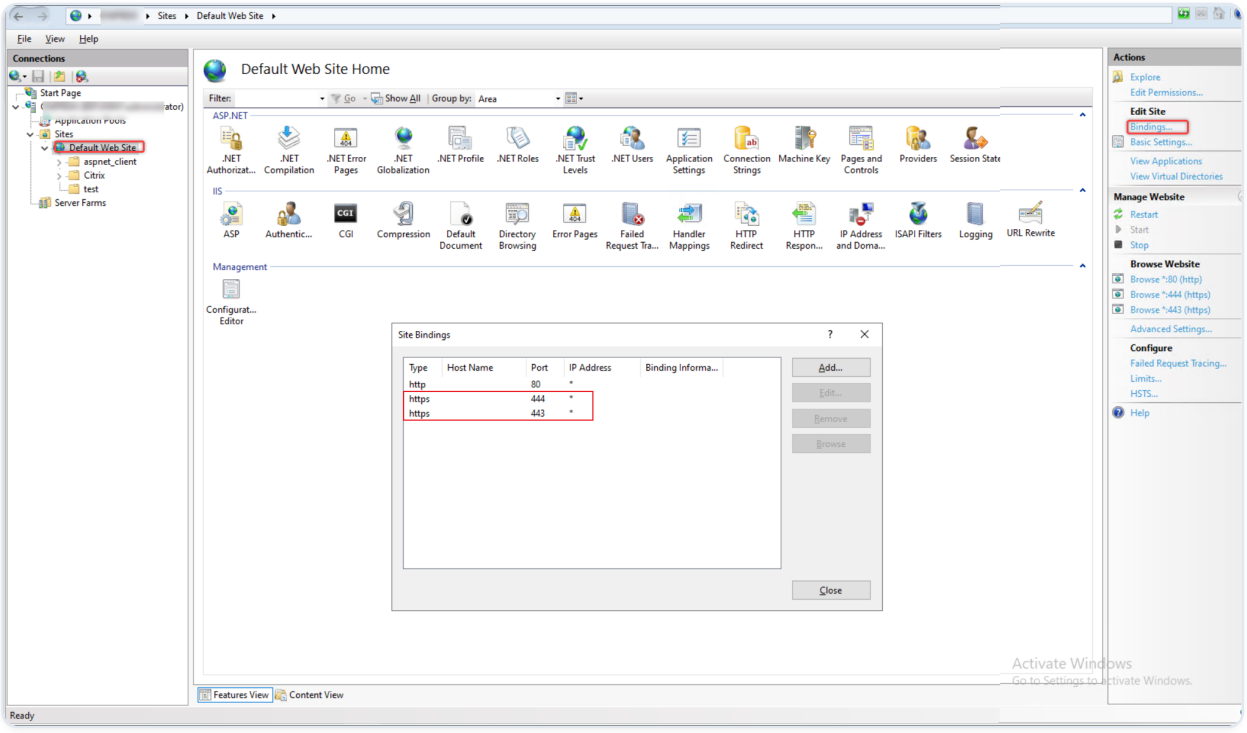



### (Opcional) Alterar o número da porta padrão

Por padrão, o Web Studio e o Director usam a porta 443 para acesso HTTPS seguro. Para alterar este número de porta, siga estas etapas para criar uma vinculação de site para a porta desejada em `Default Web Site`.

Etapas:

1. No servidor que hospeda o Web Studio, abra o **Gerenciador dos Serviços de Informações da Internet (IIS)**.
2. No painel **Conexões**, expanda o nó do servidor e selecione **Default Web Site** em **Sites**.
3. No painel **Ações** à direita, clique em **Ligações**.



4. Na janela **Ligações do Site**, clique em **Adicionar**.
5. Na janela Adicionar Ligação do Site, defina o seguinte para a nova ligação:
    a. **Tipo**: Selecione **https**.
    b. **Endereço IP**: Selecione o endereço IP apropriado ou deixe como Todos Não Atribuídos, se aplicável.
    c. **Porta**: Insira o número da porta desejado (por exemplo, 444).
    d. **Certificado SSL**: Selecione o certificado SSL apropriado para comunicação segura.

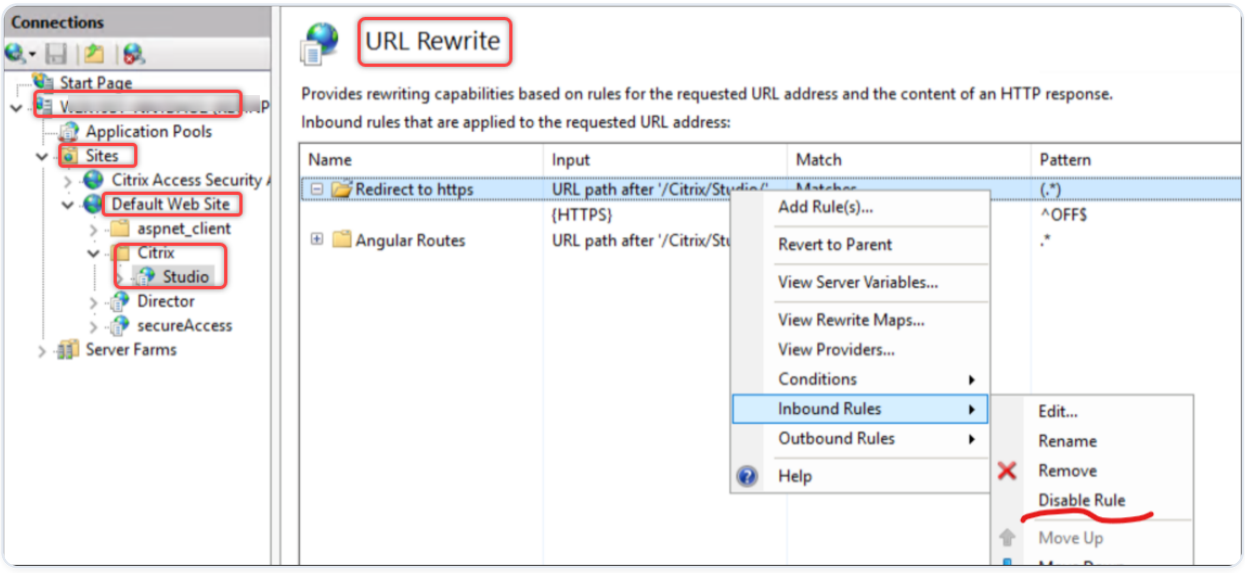
> **Nota:**
>
> Se o Delivery Controller™ e o Web Studio estiverem instalados em máquinas separadas, e o servidor não tiver outros serviços ou sites implantados, você pode remover a porta 443. Caso contrário, mantenha esta porta para evitar problemas de comunicação com o serviço de Orquestração e outros serviços FMA.

6. Clique em **OK** para salvar a vinculação e, em seguida, feche a janela **Site Bindings**.
7. No **IIS Manager**, clique no nó do servidor e, em seguida, no painel **Actions**, clique em **Restart** para aplicar a nova vinculação.

### (Opcional) Desabilitar o redirecionamento HTTPS

Ao instalar o Web Studio, por padrão, qualquer acesso HTTP é redirecionado automaticamente para HTTPS. É possível desabilitar esse redirecionamento para permitir o acesso HTTP. Essa abordagem é recomendada apenas se você tiver tomado outras medidas para bloquear o acesso HTTP. No caso de você ter um balanceador de carga de terminação TLS na frente do Web Studio, ainda é recomendado usar HTTPS entre o balanceador de carga e o Web Studio.

1. Faça logon no servidor do Web Studio.
2. Abra o **Internet Information Services (IIS) Manager** e vá para *Server_name* **> Sites > Default Web Site > URL Rewrite**.
3. Desabilite as **Inbound Rules** para **Redirection to https**, conforme mostrado na captura de tela a seguir.




Se você ativou HSTS no IIS, também deverá desmarcar **Redirect Http to Https**.

## Segurança da Camada de Transporte (TLS) no Servidor de Impressão Universal

O protocolo Transport Layer Security (TLS) é suportado para conexões baseadas em TCP entre o Virtual Delivery Agent (VDA) e o Servidor de Impressão Universal.

> **Aviso:**
>
> Para tarefas que incluem trabalhar no registro do Windows — a edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

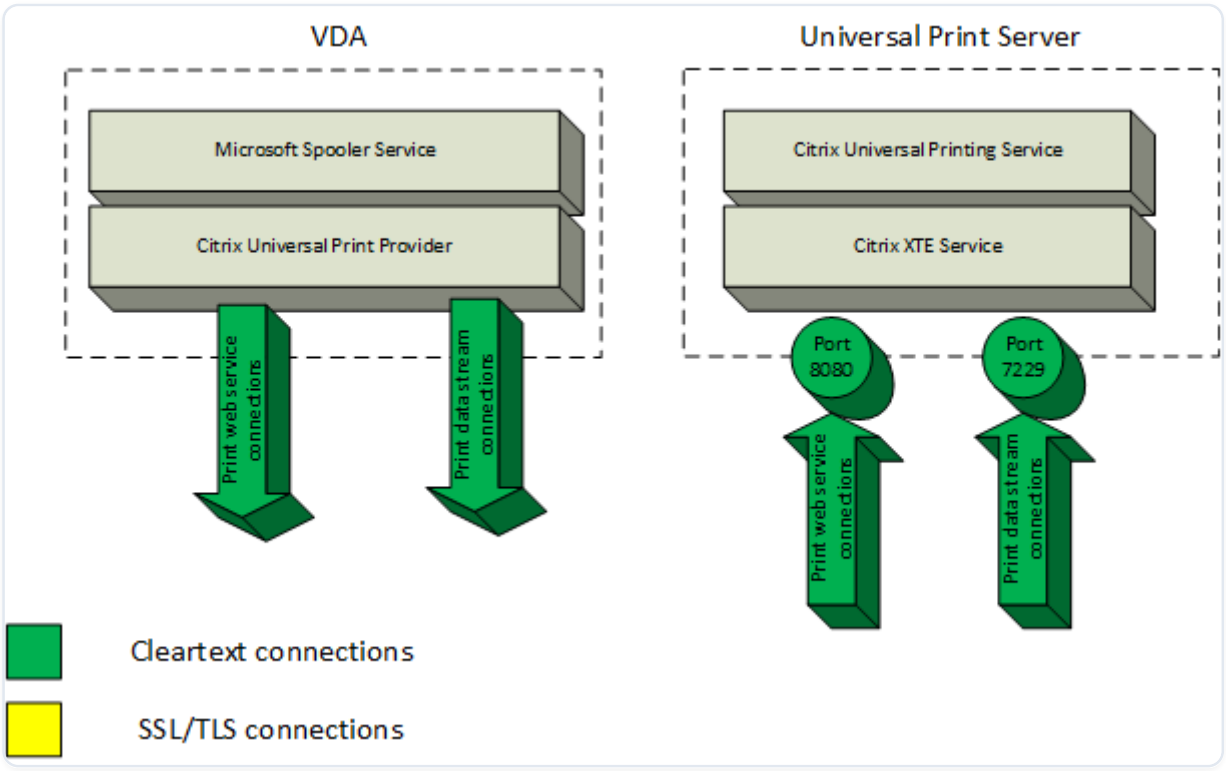
### Tipos de conexões de impressão entre o VDA e o Servidor de Impressão Universal

#### Conexões em texto não criptografado

As seguintes conexões relacionadas à impressão se originam do VDA e se conectam a portas no Servidor de Impressão Universal. Essas conexões são feitas apenas quando a configuração de política **SSL enabled** está definida como **Disabled** (o padrão).

- Conexões de serviço web de impressão em texto não criptografado (porta TCP 8080)
- Conexões de fluxo de dados de impressão em texto não criptografado (CGP) (porta TCP 7229)

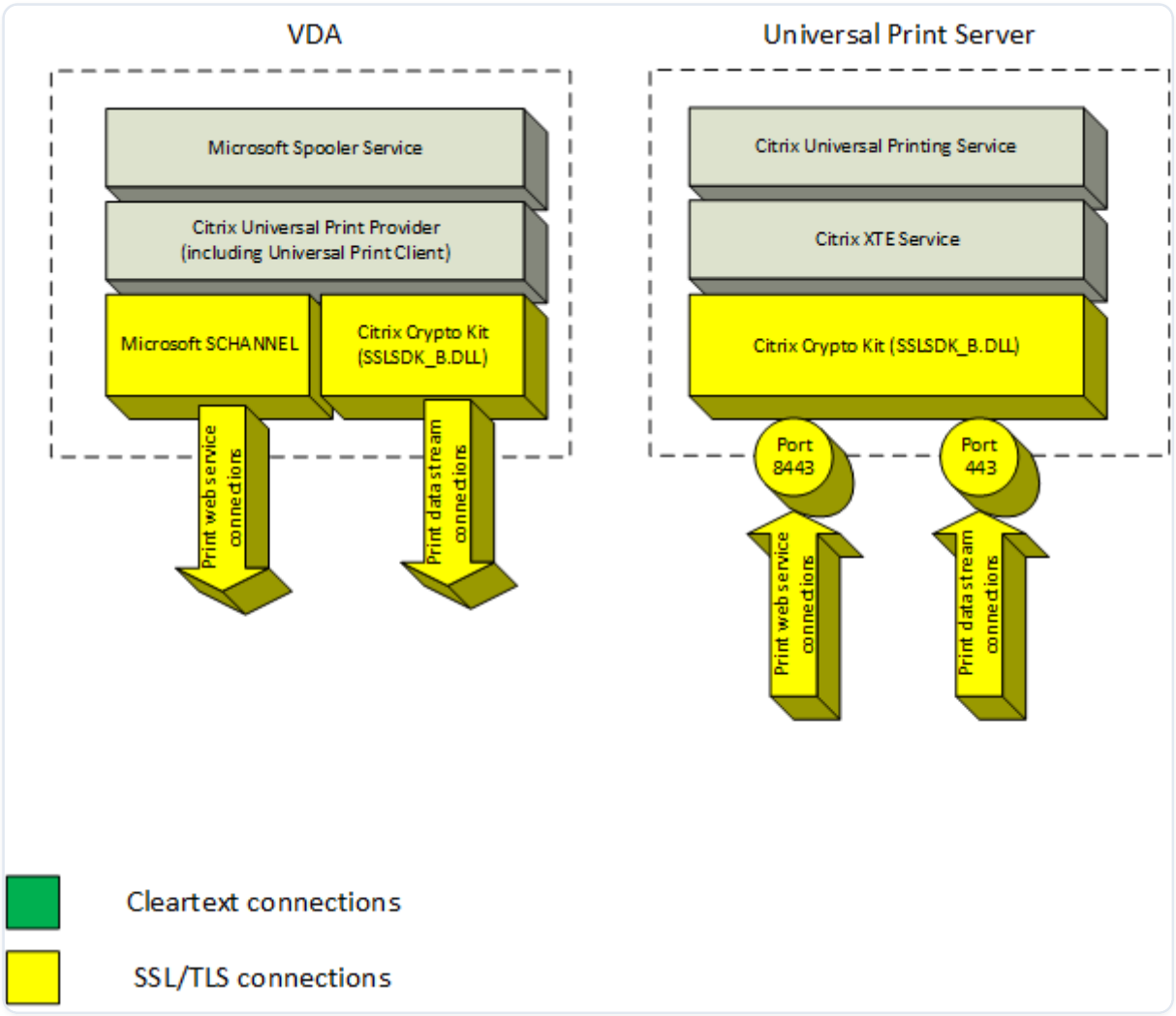
O artigo de suporte da Microsoft Service overview and network port requirements for Windows descreve as portas usadas pelo Serviço de Spooler de Impressão do Microsoft Windows. As configurações de SSL/TLS neste documento não se aplicam às conexões NetBIOS e RPC feitas pelo serviço de Spooler de Impressão do Windows. O VDA usa o Provedor de Impressão de Rede do Windows (win32spl.dll) como um fallback se a configuração de política **Universal Print Server enable** estiver definida como **Enabled with fallback to Windows' native remote printing**.




### Conexões criptografadas

Essas conexões SSL/TLS relacionadas à impressão se originam do VDA e se conectam a portas no Servidor de Impressão Universal. Essas conexões são feitas apenas quando a configuração de política **SSL enabled** está definida como **Enabled**.

- Conexões de serviço web de impressão criptografadas (porta TCP 8443)
- Conexões de fluxo de dados de impressão criptografadas (CGP) (porta TCP 443)




**Configuração do cliente SSL/TLS**

O VDA funciona como o cliente SSL/TLS.

Use a Política de Grupo da Microsoft e o registro para configurar o Microsoft SCHANNEL SSP para conexões de serviço web de impressão criptografadas (porta TCP 8443). O artigo de suporte da Microsoft Configurações de Registro TLS descreve as configurações de registro para o Microsoft SCHANNEL SSP.

Usando o Editor de Política de Grupo no VDA, vá para **Configuração do Computador > Modelos Administrativos > Rede > Configurações de Configuração SSL > Ordem do Conjunto de Cifras SSL**. Selecione a seguinte ordem quando o TLS 1.3 estiver definido:

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

Selecione a seguinte ordem quando o TLS 1.2 estiver definido:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

**Observação:**

Quando esta configuração de Política de Grupo é configurada, o VDA seleciona um conjunto de cifras para conexões de serviço web de impressão criptografadas (porta padrão: 8443) somente se as conexões aparecerem em ambas as listas de conjuntos de cifras SSL:

- Lista de ordem do conjunto de cifras SSL da Política de Grupo
- Lista correspondente à configuração de política de Conjunto de Cifras SSL selecionada (COM, GOV ou ALL)

Esta configuração de Política de Grupo também afeta outros aplicativos e serviços TLS no VDA. Se seus aplicativos exigirem conjuntos de cifras específicos, talvez seja necessário adicioná-los a esta lista de Ordem do Conjunto de Cifras da Política de Grupo.

**Importante:**

As alterações da Política de Grupo para a configuração TLS só entram em vigor após a reinicialização do sistema operacional.

Use uma política Citrix para configurar as configurações de SSL/TLS para conexões de fluxo de dados de impressão criptografados (CGP) (porta TCP 443).

### Configuração do servidor SSL/TLS

O Universal Print Server funciona como o servidor SSL/TLS.

Use o script PowerShell `Enable-UpsSsl.ps1` para configurar as definições de SSL/TLS.

### Instalar o certificado de servidor TLS no Universal Print Server

Para HTTPS, você deve instalar um certificado de servidor SSL no Universal Print Server que seja confiável para os VDAs. Use os Serviços de Certificado do Microsoft Active Directory ou outra autoridade de certificação para solicitar um certificado para o Universal Print Server.

Tenha em mente as seguintes considerações ao registrar/solicitar um certificado usando os Serviços de Certificado do Microsoft Active Directory:

1. Coloque o certificado no armazenamento de certificados **Pessoal** do Computador Local.
2. Defina o atributo **Nome Comum** do Nome Distinto do Assunto (Subject DN) do certificado para o nome de domínio totalmente qualificado (FQDN) do Universal Print Server. Especifique isso no modelo de certificado.
3. Defina o Provedor de Serviços Criptográficos (CSP) usado para gerar a solicitação de certificado e a chave privada como **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Especifique isso no modelo de certificado.
4. Defina o Tamanho da Chave para pelo menos 2048 bits. Especifique isso no modelo de certificado.

Para obter mais informações sobre como criar e instalar certificados, consulte Gerenciar certificados.

## Configurando SSL no Universal Print Server

O Serviço XTE no Universal Print Server escuta as conexões de entrada. Ele funciona como um servidor SSL quando o SSL está ativado. As conexões de entrada são de dois tipos: conexões de serviço web de impressão, que contêm comandos de impressão, e conexões de fluxo de dados de impressão, que contêm trabalhos de impressão. O SSL pode ser ativado nessas conexões. O SSL protege a confidencialidade e a integridade dessas conexões. Por padrão, o SSL está desativado.

O script PowerShell usado para configurar o SSL está na mídia de instalação e tem este nome de arquivo: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

## Configurando os números das portas de escuta no Universal Print Server

Estas são as portas padrão para o Serviço XTE:

- Porta TCP do serviço web de impressão em texto simples (HTTP): 8080
- Fluxo de dados de impressão em texto simples (CGP) porta TCP: 7229
- Serviço web de impressão criptografado (HTTPS) porta TCP: 8443
- Fluxo de dados de impressão criptografado (CGP) porta TCP: 443

Para alterar as portas usadas pelo Serviço XTE no Universal Print Server, execute os seguintes comandos no PowerShell como administrador (consulte a seção posterior para obter notas sobre o uso do script PowerShell Enable-UpsSsl.ps1):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` ou `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

### Configurações de TLS no Universal Print Server

Se você tiver vários Universal Print Servers em uma configuração de balanceamento de carga, certifique-se de que as configurações de **TLS** estejam configuradas de forma consistente em todos os Universal Print Servers.

Ao configurar o TLS no Universal Print Server, as permissões no certificado TLS instalado são alteradas, concedendo ao Serviço de Impressão Universal acesso de leitura à chave privada do certificado e informando ao Serviço de Impressão Universal o seguinte:

- Qual certificado no armazenamento de certificados usar para TLS.
- Quais números de porta TCP usar para conexões TLS.

O Firewall do Windows (se ativado) deve ser configurado para permitir conexões de entrada nessas portas TCP. Essa configuração é feita automaticamente quando você usa o script PowerShell Enable-UpsSsl.ps1.

- Quais versões do protocolo TLS permitir.

O Universal Print Server suporta as versões 1.3 e 1.2 do protocolo TLS. Especifique a versão mínima permitida.

A versão padrão do protocolo TLS é 1.2.

> **Observação:**
>
> TLS 1.1 e 1.0 não são mais suportados a partir da versão 2311 do Citrix Virtual Apps and Desktops.

- Quais conjuntos de cifras TLS permitir.

Um conjunto de cifras seleciona os algoritmos criptográficos que são usados para uma conexão. VDAs e o Universal Print Server podem suportar diferentes conjuntos de cifras. Quando um VDA se conecta e envia uma lista de conjuntos de cifras TLS suportados, o Universal Print Server compara um dos conjuntos de cifras do cliente com um dos conjuntos de cifras em sua própria lista de conjuntos de cifras configurados e aceita a conexão. Se não houver um conjunto de cifras correspondente, o Universal Print Server rejeita a conexão.

O Universal Print Server suporta os seguintes conjuntos de cifras nomeados GOV(ernment), COM(mercial) e ALL para os modos de Crypto Kit nativo OPEN, FIPS e SP800-52. Os conjuntos de cifras aceitáveis também dependem da configuração da política **Modo FIPS SSL** e do Modo FIPS do Windows. Consulte este artigo de suporte da Microsoft para obter informações sobre o modo FIPS do Windows.

| CONJUNTO DE CIFRAS (EM ORDEM DECRESCENTE DE PRIORIDADE) | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| TLS_ECDHE_RSA_AES256_GCM_SHA384 | X | | X | X | | X | X | | X |
| TLS_ECD | X | | X | X | | X | X | | X |

| CONJUNTO DE CIFRAS (EM ORDEM DECRESCENTE DE PRIORIDADE) | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| HE_RSA_AES256_CBC_SHA384 | | | | | | | | | |
| TLS_ECDHE_RSA_AES256_CBC_SHA | X | X | | X | X | | X | X | |

### Configurar TLS em um Universal Print Server usando o script PowerShell

Instale o Certificado TLS na área **Computador Local > Pessoal > Certificados** do armazenamento de certificados. Se mais de um certificado residir nesse local, forneça a impressão digital do certificado para o script PowerShell `Enable-UpsSsl.ps1`.

> **Observação:**

O script PowerShell encontra o certificado correto com base no FQDN do Universal Print Server. Você não precisa fornecer a impressão digital do certificado quando apenas um único certificado está presente para o FQDN do Universal Print Server.

O script `Enable-UpsSsl.ps1` habilita ou desabilita conexões TLS originadas do VDA para o Universal Print Server. Este script está disponível na pasta **Support > Tools > SslSupport** na mídia de instalação.

Ao habilitar o TLS, o script desabilita todas as regras existentes do Firewall do Windows para as portas TCP do Universal Print Server. Em seguida, ele adiciona novas regras que permitem que o Serviço XTE aceite conexões de entrada apenas nas portas TCP e UDP TLS. Ele também desabilita as regras do Firewall do Windows para:

- Conexões de serviço web de impressão em texto simples (padrão: 8080)
- Conexões de fluxo de dados de impressão em texto simples (CGP) (padrão: 7229)

O efeito é que o VDA pode fazer essas conexões apenas ao usar TLS.

**Observação:**

A habilitação do TLS não afeta as conexões RPC/SMB do Spooler de Impressão do Windows originadas do VDA e destinadas ao Universal Print Server.

**Importante:**

Especifique **Enable** ou **Disable** como o primeiro parâmetro. O parâmetro CertificateThumbprint é opcional se apenas um certificado no armazenamento de certificados Pessoal do Computador Local tiver o FQDN do Universal Print Server. Os outros parâmetros são opcionais.

**Sintaxe**

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-
HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;]
[-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-
FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]
```

```
Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum>] [-CGPPort
&lt;portnum>]
```

| PARÂMETRO | DESCRIÇÃO |
|---|---|
| Habilitar | Habilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Disable é obrigatório. |
| Desabilitar | Desabilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Enable é obrigatório. |
| ImpressãoDigitalDoCertificado `"<thumbprint>"` | Impressão digital do certificado TLS no armazenamento de certificados Pessoal do Computador Local, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar. |
| PortaHTTP `<port>` | Porta do serviço web de impressão em texto simples (HTTP/SOAP). Padrão: 8080 |
| PortaCGP `<port>` | Porta do fluxo de dados de impressão em texto simples (CGP). Padrão: 7229 |
| PortaHTTPS `<port>` | Porta do serviço web de impressão criptografado (HTTPS/SOAP). Padrão: 8443 |
| PortaCGPSSL `<port>` | Porta do fluxo de dados de impressão criptografado (CGP). Padrão: 443 |
| VersãoMínimaSSL `"<version>"` | Versão mínima do protocolo TLS, entre aspas. Valores válidos: "TLS_1.2" e "TLS_1.3". Padrão: TLS_1.2. |
| ConjuntoDeCifrasSSL `"<name>"` | Nome do pacote de conjunto de cifras TLS, entre aspas. Valores válidos: "GOV", "COM" e "ALL" (padrão). |
| ModoFIPS `<Boolean>` | Habilita ou desabilita o modo FIPS 140 no Servidor XTE. Valores válidos: $true para |

| PARÂMETRO | DESCRIÇÃO |
| --- | --- |
| | habilitar o modo FIPS 140, $false para desabilitar o modo FIPS 140. |

#### Exemplos

O script a seguir habilita o TLS. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

O script a seguir desabilita o TLS.

```
Enable-UpsSsl.ps1 –Disable
```

### Configurando o modo FIPS

A habilitação do modo FIPS (US Federal Information Processing Standards) garante que apenas criptografia compatível com FIPS 140 seja usada para conexões criptografadas do Universal Print Server.

Configure o modo FIPS no servidor antes de configurar o modo FIPS no cliente.

Consulte o site de documentação da Microsoft para habilitar/desabilitar o modo FIPS do Windows.

#### Habilitando o modo FIPS no cliente

No Delivery Controller™, execute o Web Studio e defina a configuração da política Citrix **Modo FIPS do UPS** como **Habilitado**. Habilite a política Citrix.

Faça isso em cada VDA:

1. Habilite o modo FIPS do Windows.
2. Reinicie o VDA.

#### Habilitando o modo FIPS no servidor

Faça isso em cada Universal Print Server:

1. Habilite o modo FIPS do Windows.
2. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $true`.

4. Reinicie o Universal Print Server.

#### Desabilitando o modo FIPS no cliente

No Web Studio, defina a configuração da política Citrix **Modo FIPS do UPS** como **Desativado**. Habilite a política Citrix. Você também pode excluir a configuração da política Citrix **Modo FIPS do UPS**.

Faça isso em cada VDA:

1. Desabilite o modo FIPS do Windows.
2. Reinicie o VDA.

#### Desabilitando o modo FIPS no servidor

Faça isso em cada Universal Print Server:

1. Desabilite o modo FIPS do Windows.
2. Execute este comando do PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $false`.
4. Reinicie o Universal Print Server.

> **Observação:**
>
> O modo FIPS não é compatível quando a versão do protocolo SSL está definida como TLS 1.3.

### Configurando a versão do protocolo SSL/TLS

A versão padrão do protocolo SSL/TLS é TLS 1.2. TLS 1.2 e TLS 1.3 são as versões de protocolo SSL/TLS recomendadas para uso em produção. Para solução de problemas, pode ser necessário alterar temporariamente a versão do protocolo SSL/TLS em um ambiente que não seja de produção.

SSL 2.0 e SSL 3.0 não são suportados no Universal Print Server.

#### Definindo a versão do protocolo SSL/TLS no servidor

No Studio, defina a configuração de política **SSL Protocol Version** para a versão de protocolo desejada e ative a política.

Certifique-se de que o sistema operacional do VDA suporte a versão TLS selecionada. Para versões TLS suportadas no Windows, consulte Microsoft Learn - TLS protocol version support. Para configurar o registro para substituir os padrões, consulte Microsoft Learn - TLS, DTLS, and SSL protocol version settings.

#### Definindo a versão do protocolo SSL/TLS no cliente

Faça isso em cada VDA:

1. No Delivery Controller, defina a configuração de política **SSL Protocol Version** para a versão de protocolo desejada e ative a política.
2. O artigo de suporte da Microsoft TLS Registry Settings descreve as configurações de registro para o Microsoft SCHANNEL SSP. Habilite o **TLS 1.2 ou TLS 1.3** do lado do cliente usando as configurações de registro.

   > **Importante:**
   >
   > Lembre-se de restaurar as configurações do registro para seus valores originais quando terminar os testes.

3. Reinicie o VDA.

### Solução de problemas

Se ocorrer um erro de conexão, verifique o arquivo C:\Program Files (x86)\Citrix\XTE\logs\error.log no Universal Print Server.

A mensagem de erro **SSL handshake from client failed** aparece neste arquivo de log se o handshake SSL/TLS falhar. Tais falhas podem ocorrer se a versão do protocolo SSL/TLS no VDA e no Universal Print Server não corresponderem.

Use o FQDN do Universal Print Server nas seguintes configurações de política que contêm nomes de host do Universal Print Server:

- Impressoras de sessão
- Atribuições de impressora
- Servidores de Impressão Universal para balanceamento de carga

Certifique-se de que o relógio do sistema (data, hora e fuso horário) estejam corretos nos Servidores de Impressão Universal e nos VDAs.

# Lista de permissão de canal virtual

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas os canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

## Configuração

A lista de permissões de canal virtual é habilitada por padrão. Você pode configurar esse recurso usando as seguintes configurações na política Citrix:

- **Lista de permissão de canal virtual**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.
- **Limitação de log da lista de permissão de canal virtual**: define o período de limitação para o registro de eventos da lista de permissão de canal virtual.
- **Registro em log da lista de permissão de canal virtual**: define o nível de registro em log para a lista de permissão de canal virtual.

## Adicionando canais virtuais à lista de permissão

Para adicionar um canal virtual à lista de permissão, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissão usando a configuração de política da lista de permissão de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

### Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

### Para múltiplos processos

Se houver múltiplos processos, adicione a seguinte entrada à lista:

`CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe`

### Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`
- Todos os caminhos devem ser locais.

> **Nota:**

- Caminhos de rede não são permitidos.
- O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
- O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

### Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

**Nota:**

Variáveis de ambiente do usuário não são suportadas.

O suporte a variáveis de ambiente está disponível a partir da versão 2209 do Citrix Virtual Apps and Desktops.

## Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política de lista de permissões de canais virtuais para o canal virtual e o processo identificados.
5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

## Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- Pacote de Otimização HDX RealTime para Skype for Business

### Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`
- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.

- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### Pacote de Otimização HDX RealTime para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

# Comunicação WebSocket entre VDA e Delivery Controller™

Este artigo descreve como configurar uma conexão WebSocket para comunicação entre VDAs e Delivery Controllers.

## Visão geral

O protocolo WebSocket funciona sobre o Protocolo de Brokering Citrix e facilita a comunicação estável entre Delivery Controllers e VDAs. O uso do protocolo WebSocket para comunicação oferece os seguintes benefícios:

- Requer apenas a porta TLS 443 para comunicação do VDA para o Delivery Controller.
- Fornece canais de comunicação contínuos e confiáveis entre VDAs e Delivery Controllers.

## Como funciona

A seção a seguir descreve o fluxo de trabalho para a conexão WebSocket entre um Delivery Controller e um VDA:

1. Os administradores do Citrix Virtual Apps and Desktops™ iniciam o processo provisionando VDAs usando o Machine Creation Service (MCS).
2. Durante o processo de provisionamento do MCS, o MCS gera pares de chaves pública-privada para cada VDA e registra as chaves públicas com o serviço de confiança FMA no Delivery Controller. O MCS salva o par de chaves pública-privada como um arquivo no disco de identidade nos VDAs.

3. Quando a máquina VDA inicializa, o agente MCS instalado na máquina VDA lê o par de chaves do disco de identidade e grava essas informações no local do registro do VDA.
4. O agente de broker instalado no VDA lê os pares de chaves do registro e gera uma solicitação WebSocket habilitada para SSL para o Delivery Controller com a chave de serviço assinada pela chave privada.
5. O Delivery Controller verifica o cabeçalho de autorização da chave de serviço assinada com a chave pública do serviço de confiança FMA.
6. Concluída a verificação, o sistema estabelece a conexão WebSocket entre o VDA e o Delivery Controller.

## Suporte WebSocket para VDAs ingressados no AD

### Antes de começar

1. Configure seu site. Para obter mais informações, consulte Criar um site.
2. Instale certificados TLS nos Delivery Controllers. Para obter mais informações, consulte Instalar certificados de servidor TLS nos Controllers.
3. Instale a CA raiz e a CA intermediária no VDA para confiar no Delivery Controller.

### Procedimento

Siga as instruções para configurar uma conexão WebSocket:

1. Habilite a conexão WebSocket no Delivery Controller. Execute o seguinte comando em cada Delivery Controller presente em seu site:

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   > **Observação:**
   >
   > Certifique-se de reiniciar os Delivery Controllers após habilitar o WebSocket.

2. Crie um catálogo de máquinas para VDAs unidos ao AD com provisionamento MCS. Para obter mais informações, consulte Criar catálogo de máquinas.
3. Crie um grupo de entrega e adicione seu VDA a ele. Para obter mais informações, consulte Criar grupos de entrega.

4. Habilite a conexão WebSocket no VDA. Execute o seguinte comando no VDA:

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

- Para verificar se o VDA está conectado ao servidor via WebSocket, verifique o seguinte valor da chave de registro.

  Chave:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  Nome: Conectado

  Tipo: REG_DWORD

  Valor: 1 ou 0

  1: VDA conectado ao servidor usando WebSocket.

  0: O VDA não consegue alcançar o servidor via WebSocket ou o WebSocket não está ativado.

- Para verificar se o WebSocket está ativado, verifique o seguinte valor da chave de registro. O valor de `Enabled` deve ser 1.

  Chave:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  Nome: Habilitado

  Tipo: REG_DWORD

  Valor: 1

# Conectividade HDX™

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

O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

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

Dentro da oferta HDX, você pode se conectar por meio de um protocolo de transporte exclusivo e proprietário, utilizar as unidades máximas de transmissão ao estabelecer sessões e otimizar a conectividade com o Citrix SD-WAN.

## Transporte adaptável

O Transporte Adaptável é um mecanismo no Citrix Virtual Apps and Desktops™ que permite estabelecer conexões para sessões HDX usando um protocolo de transporte preferencial, enquanto oferece uma alternativa para TCP se a conectividade com o protocolo preferencial não estiver disponível.

Os seguintes protocolos de transporte são suportados:

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

### Configuração

O Transporte Adaptável está ativado por padrão. Você pode configurar o Transporte Adaptável para operar nos seguintes modos:

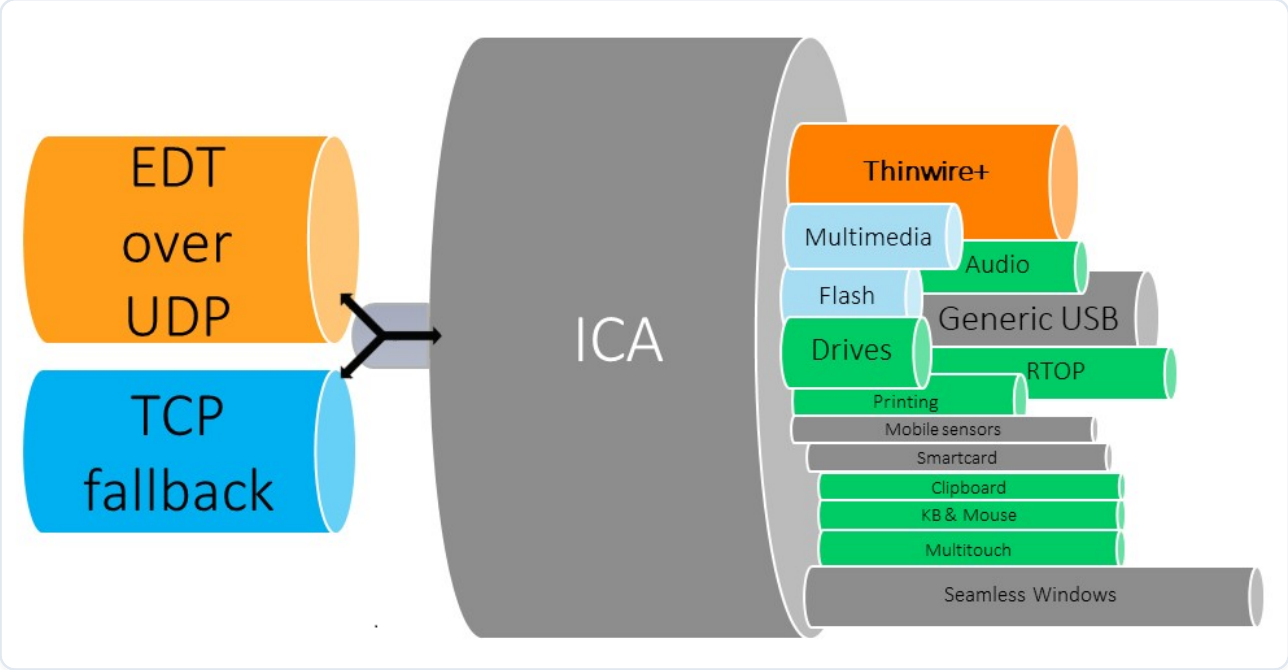
- **Preferencial**: (Padrão) O cliente tenta se conectar com o protocolo preferencial e retorna para TCP se a conectividade com o protocolo preferencial não estiver disponível.
- **Modo de diagnóstico**: O cliente tenta se conectar apenas usando o protocolo preferencial. O retorno para TCP está desativado.
- **Desativado**: O cliente tenta se conectar apenas usando TCP.

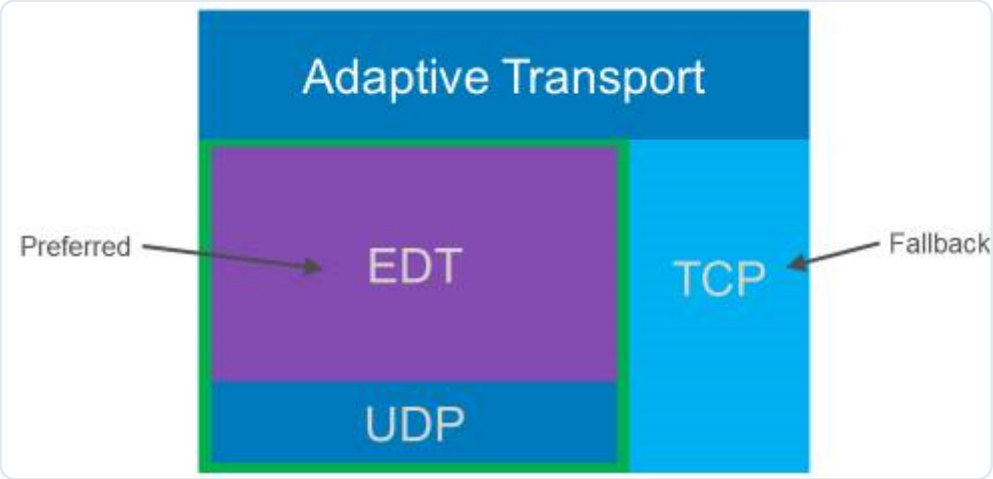
## Como funciona

Quando o **Transporte Adaptável** está definido como `Preferred`, o cliente tenta se conectar à sessão com o protocolo preferencial e TCP em paralelo. Isso permite otimizar o tempo de conexão se não for possível conectar com o protocolo preferencial e o cliente precisar retornar para TCP. Se a conexão for estabelecida usando TCP, o cliente tenta se conectar com o protocolo preferencial em segundo plano a cada cinco minutos.

Quando o **Transporte Adaptável** está definido como `Diagnostic mode`, o cliente se conecta à sessão apenas com o protocolo preferencial. Se o cliente não conseguir estabelecer uma conexão usando o protocolo preferencial, ele não retorna para TCP, e a conexão falha.

Quando o **Transporte Adaptável** está definido como `Off`, o **Transporte Adaptável** é desativado, e o cliente se conecta à sessão usando apenas TCP.






## Requisitos do sistema

A seguir estão os requisitos para usar o Transporte Adaptável e EDT:

- Plano de controle
  - Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops)
  - Citrix Virtual Apps and Desktops: versão atualmente suportada
- Agente de Entrega Virtual
  - Windows: versão atualmente suportada (2402 ou posterior é recomendada)
  - Linux: versão atualmente suportada (2402 ou posterior é recomendada)
- Aplicativo Citrix Workspace™
  - Windows: versão atualmente suportada (2402 ou posterior é recomendada)
  - Linux: versão atualmente suportada (2402 ou posterior é recomendada)
  - Mac: versão atualmente suportada (2402 ou posterior é recomendada)
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível no Google Play
- Citrix NetScaler® Gateway
  - 14.1.12.30 ou posterior (recomendado)
  - 13.1.17.42 ou posterior (13.1-52.19 ou posterior recomendado)

> **Observação:**

Para obter detalhes sobre o VDA Linux, consulte a documentação do Agente de Entrega Virtual Linux.

## Requisitos de rede

As seções a seguir são os requisitos de rede para usar o EDT com o Adaptive Transport:

### Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deverá permitir o seguinte tráfego de entrada para conexões internas.

| DESCRIÇÃO | ORIGEM | PROTOCOLO | PORTA |
|---|---|---|---|
| Conexão interna - Confiabilidade da sessão ativada | Cliente | UDP | 2598 |
| Conexão interna - Confiabilidade da sessão desativada | | | 1494 |
| Conexão interna - HDX™ Direct ou VDA SSL | | | 443 |

**Observação:**

O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

### Rede interna

A tabela a seguir descreve as regras de firewall necessárias para usar o EDT em sua rede:

| DESCRIÇÃO | PROTOCOLO | ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|
| Conexão interna direta - Confiabilidade | UDP | Rede do cliente | Rede VDA | 2598 |

| DESCRIÇÃO | PROTOCOLO | ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|
| da sessão ativada | | | | |
| Conexão interna direta - Confiabilidade da sessão desativada | | | | 1494 |
| Conexão interna direta - HDX Direct ou VDA SSL | | | | 443 |
| NetScaler Gateway | | NetScaler SNIP | | 2598 |
| NetScaler Gateway - VDA SSL | | | | 443 |

**Observação:**

Se você estiver usando o Citrix Gateway Service, você deve habilitar o **Rendezvous** para usar o EDT como seu protocolo de transporte. Consulte a documentação Rendezvous para requisitos de sistema e rede.

### Rede do cliente

A tabela a seguir descreve os requisitos de conectividade para dispositivos cliente:

| DESCRIÇÃO | PROTOCOLO | ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|
| Conexão interna - Confiabilidade | UDP | IP do cliente | Rede VDA | 2598 |

| DESCRIÇÃO | PROTOCOLO | ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|
| da sessão habilitada | | | | |
| Conexão interna - Confiabilidade da sessão desabilitada | | | | 1494 |
| Conexão interna - HDX Direto ou SSL VDA | | | | 443 |
| Conexão externa - NetScaler Gateway | | | Endereço IP público do NetScaler Gateway | 443 |
| Conexão externa - Citrix Gateway Service | | | Citrix Gateway Service | 443 |

**Observação:**

Se você estiver usando o Citrix Gateway Service, os clientes devem ser capazes de alcançar `<https://*.*.nssvc.net>`. Se você não puder permitir todos os subdomínios usando `<https://*.*.nssvc.net>`, você pode usar `<https://*.c.nssvc.net>` e `<https://*.g.nssvc.net>` em vez disso. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX270584.

## Transporte de Dados Iluminado

Enlightened Data Transport (EDT) é um protocolo de transporte proprietário da Citrix construído sobre o User Datagram Protocol (UDP). Ele oferece uma experiência de usuário superior em conexões de longa distância desafiadoras, mantendo a escalabilidade do servidor. O EDT melhora

o rendimento de dados para todos os canais virtuais ICA® em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.

Quando o **Transporte Adaptável** está ativado, o EDT é o protocolo preferencial.

### Coisas a saber

- A **Confiabilidade da Sessão** deve estar ativada para usar a **Descoberta de MTU** e o EDT com o NetScaler® Gateway e o Citrix Gateway Service.
- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha na abertura de sessões em alguns casos. Para evitar isso, você deve ajustar o MTU do EDT para um valor adequado às suas redes. Você pode usar a Descoberta de MTU do EDT ou uma solução alternativa manual descrita em Como configurar o MSS ao usar o EDT em redes com MTU não padrão.
- Para obter detalhes sobre como habilitar o uso do EDT com o NetScaler Gateway, consulte Configurar o NetScaler Gateway para oferecer suporte ao Enlightened Data Transport.

### Descoberta de MTU do EDT

A Descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso evita a fragmentação de pacotes EDT que pode resultar em degradação do desempenho ou falha no estabelecimento de uma sessão.

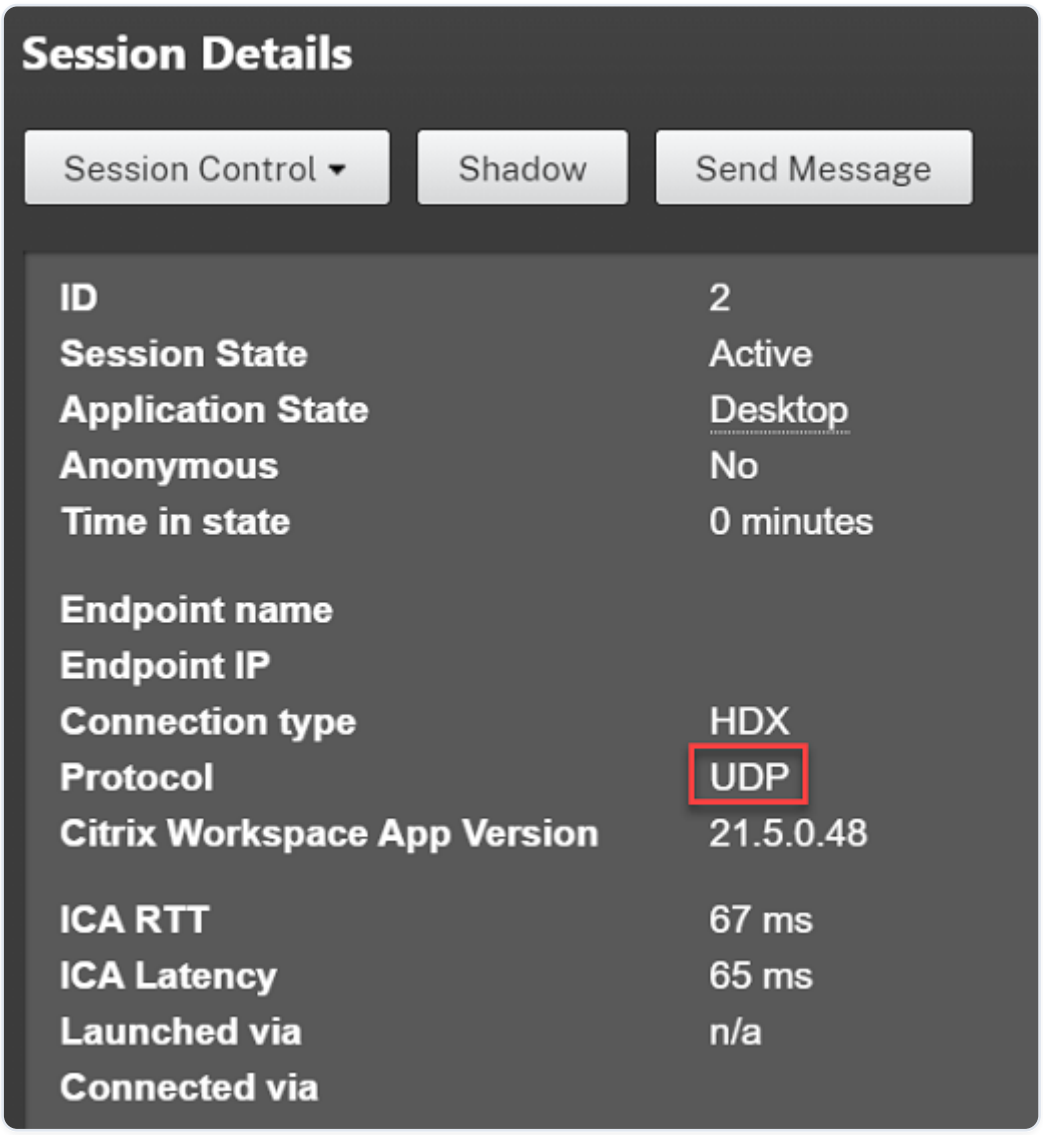
A Descoberta de MTU está ativada por padrão. Se precisar desativá-la, consulte Recursos HDX gerenciados através do registro para obter detalhes.

> **Nota:**
>
> - A **Confiabilidade da Sessão** deve estar ativada para que a Descoberta de MTU funcione.
> - A Descoberta de MTU com Multi-Stream ICA está disponível com as versões 2209 e posteriores do VDA.

## Solução de problemas

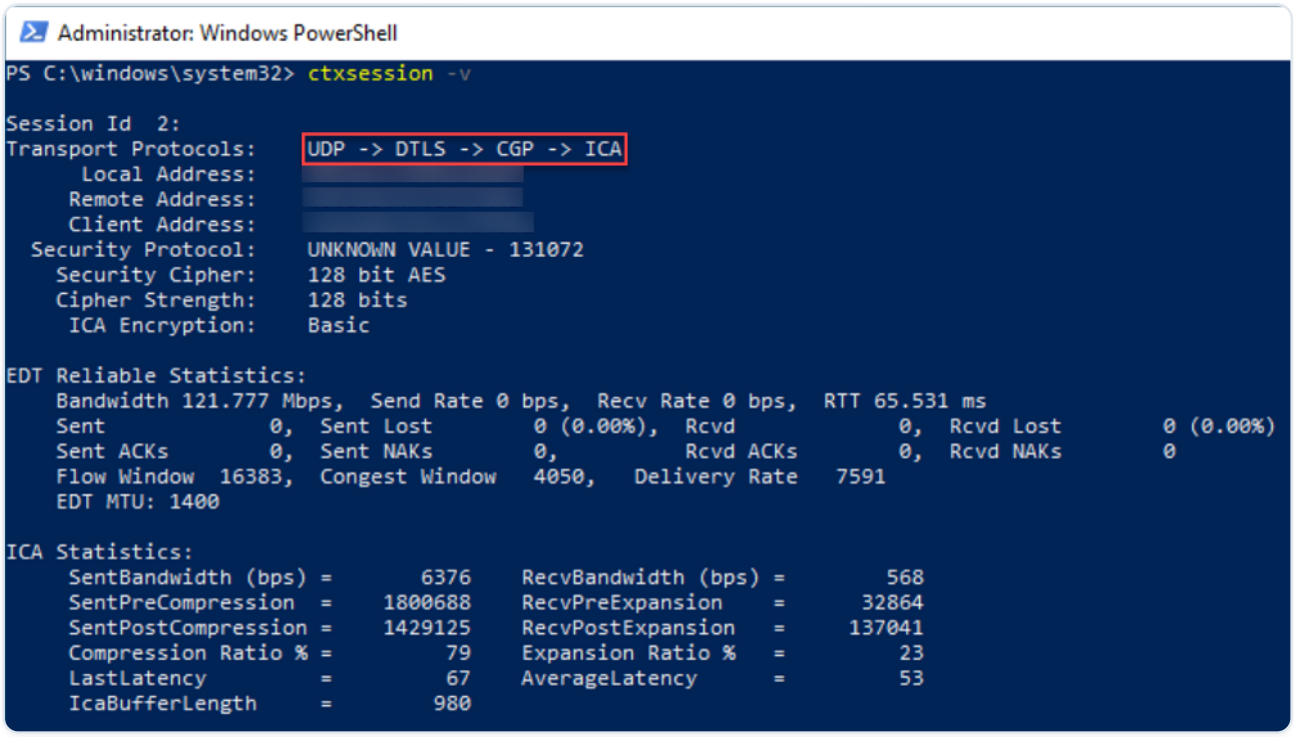
Para confirmar que o EDT está sendo usado como protocolo de transporte para a sessão, você pode usar o Director ou o utilitário de linha de comando `CtxSession.exe` no VDA.

No Director, procure a sessão e selecione **Detalhes**. Se o **Tipo de conexão** for `HDX` e o **Protocolo** for `UDP`, o EDT está sendo usado como protocolo de transporte para a sessão.




Para usar o utilitário CtxSession.exe, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe`. Para ver estatísticas detalhadas, execute `ctxsession.exe -v`. Se o EDT estiver em uso, o protocolo de transporte mostrará um dos seguintes:

- **UDP > ICA®** (Confiabilidade da sessão desabilitada)
- **UDP > CGP > ICA** (Confiabilidade da sessão habilitada)
- **UDP > DTLS > CGP > ICA** (ICA é criptografado de ponta a ponta com DTLS)




### Quando as sessões falham ao conectar com EDT

Para solucionar problemas de **Transporte Adaptável** e **EDT**, sugerimos o seguinte:

1. Revise os Requisitos do sistema, Requisitos de rede, Problemas conhecidos e Coisas a saber, e certifique-se de que todos os itens foram abordados.
2. Verifique se há políticas Citrix® no Studio ou GPO substituindo a configuração desejada de **Transporte Adaptável HDX**.
3. Verifique se há configurações no cliente substituindo a configuração desejada de Transporte Adaptável HDX. Isso pode ser uma preferência de GPO, uma configuração usando o modelo administrativo opcional do aplicativo Workspace ou uma configuração manual da configuração **HDXoverUDP** no registro ou no arquivo de configuração do cliente.
4. Em máquinas VDA de várias sessões, certifique-se de que os ouvintes UDP estejam ativos. Abra um prompt de comando na máquina VDA e execute `netstat -a -p udp`. Para obter mais informações, consulte Como confirmar o protocolo de transporte de dados iluminado HDX.
5. Verifique se as regras de firewall apropriadas foram configuradas tanto nos firewalls de rede quanto nos firewalls em execução nas máquinas VDA.
6. Inicie uma sessão direta internamente, ignorando o NetScaler® Gateway ou o Citrix Gateway Service, e verifique o protocolo em uso. Se a sessão usar EDT, o VDA estará pronto para usar EDT para conexões externas através do NetScaler Gateway ou do Citrix Gateway Service.

7. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo NetScaler Gateway ou Citrix Gateway Service:
    - Certifique-se de que a **Confiabilidade da Sessão** esteja ativada.
    - Se estiver usando o NetScaler Gateway, certifique-se de que sua configuração esteja de acordo com a configuração necessária descrita em Configurar o NetScaler Gateway para oferecer suporte ao Enlightened Data Transport e ao HDX Insight.
8. Se estiver usando o Citrix Gateway Service, certifique-se de que o Rendezvous esteja ativado e funcionando.
9. Verifique se as conexões dos seus usuários exigem um MTU não padrão. Conexões com um MTU efetivo inferior a 1500 bytes causam fragmentação de pacotes EDT, o que, por sua vez, pode afetar o desempenho ou até mesmo causar falhas no lançamento da sessão. Esse problema é comum ao usar VPNs, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Certifique-se de ter a Descoberta de MTU ativada ou de estar configurando um MTU personalizado conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

### Problemas conhecidos

- Caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe para conexões que não passam pelo NetScaler Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para a versão 2103 ou posterior do VDA.
- Ao usar o NetScaler Gateway, caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe. Isso ocorre devido a um problema no Gateway que faz com que o bit Don’t Fragment (DF) no cabeçalho dos pacotes EDT não seja propagado. Uma correção para esse problema está disponível, a partir da versão de firmware 13.1 build 17.42. Para obter detalhes sobre como ativar a correção, consulte a documentação do NetScaler Gateway.
- A Descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não respeitam o bit DF quando o processamento de pacotes está ativado, impedindo que a Descoberta de MTU detecte a fragmentação. Nesta situação, as seguintes opções estão disponíveis:
    - Desative o processamento de pacotes no modem do usuário.
    - Desative a **Descoberta de MTU** e use um MTU codificado, conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

- Desative o **Transporte Adaptável** para forçar as sessões a usar TCP. Se apenas um subconjunto de usuários for afetado, considere desativá-lo no lado do cliente para que outros usuários possam continuar a usar o EDT.

# HDX™ Direct

Ao acessar recursos fornecidos pela Citrix, o HDX Direct permite que dispositivos cliente internos e externos estabeleçam uma conexão direta segura com o host da sessão, se a comunicação direta for possível.

## Requisitos do sistema

A seguir estão os requisitos de sistema para usar o HDX Direct:

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2503 ou posterior
- Aplicativo Workspace
  - Windows: versão 2503 ou posterior
  - Linux: versão 2411 ou posterior
  - Mac: versão 2411 ou posterior
- Camada de acesso
  - Citrix Workspace™
  - Citrix Storefront™ 2503 ou posterior
  - Citrix Gateway Service
  - Citrix NetScaler® Gateway

## Requisitos de rede

A seguir estão os requisitos de rede para usar o HDX Direct.

### Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deverá permitir o seguinte tráfego de entrada para conexões internas.

| DESCRIÇÃO | ORIGEM | PROTOCOLO | PORTA |
|---|---|---|---|
| Conexão interna direta | Cliente | TCP | 443 |
| Conexão interna direta | Cliente | UDP | 443 |

> Nota:
>
> O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

### Rede do cliente

A tabela a seguir descreve a rede do cliente para usuários internos e externos.

#### Usuários internos

| DESCRIÇÃO | PROTOCOLO | ORIGEM | PORTA DE ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|---|
| Conexão interna direta | TCP | Rede do cliente | 1024–65535 | Rede VDA | 443 |
| Conexão interna direta | UDP | Rede do cliente | 1024–65535 | Rede VDA | 443 |

### Usuários externos

| DESCRIÇÃO | PROTOCOLO | ORIGEM | PORTA DE ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|---|
| STUN (somente usuários externos) | UDP | Rede do cliente | 1024–65535 | Internet (consulte a nota abaixo) | 3478, 19302 |
| Conexão de usuário externo | UDP | Rede do cliente | 1024–65535 | Endereço IP público do data center | 1024–65535 |

## Rede do data center

A tabela a seguir descreve a rede do data center para usuários internos e externos.

### Usuários internos

| DESCRIÇÃO | PROTOCOLO | ORIGEM | PORTA DE ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|---|
| Conexão interna direta | TCP | Rede do cliente | 1024–65535 | Rede VDA | 443 |
| Conexão interna direta | UDP | Rede do cliente | 1024–65535 | Rede VDA | 443 |

### Usuários externos

| DESCRIÇÃO | PROTOCOLO | ORIGEM | PORTA DE ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|---|
| STUN (somente usuários externos) | UDP | Rede VDA | 1024–65535 | Internet (veja a observação abaixo) | 3478, 19302 |
| Conexão de usuário externo | UDP | DMZ / Rede interna | 1024–65535 | Rede VDA | 55000–55250 |

| DESCRIÇÃO | PROTOCOLO | ORIGEM | PORTA DE ORIGEM | DESTINO | PORTA DE DESTINO |
|---|---|---|---|---|---|
| Conexão de usuário externo | UDP | Rede VDA | 55000–55250 | IP público do cliente | 1024–65535 |

**NOTA:**

Tanto o VDA quanto o aplicativo Workspace tentam enviar solicitações STUN para os seguintes servidores na mesma ordem:

- stun.cloud.com:3478
- stun.cloudflare.com:3478
- stun.l.google.com:19302

Se você alterar o intervalo de portas padrão para conexões de usuários externos usando a configuração de política **Intervalo de portas do HDX Direct**, as regras de firewall correspondentes devem corresponder ao seu intervalo de portas personalizado.

## Configuração

O HDX Direct está desabilitado por padrão. Você pode configurar este recurso usando a configuração **HDX Direct** na política do Citrix.

- **HDX Direct**: Para habilitar ou desabilitar um recurso.
- **Modo HDX Direct**: Determina se o **HDX Direct** está disponível apenas para clientes internos ou para clientes internos e externos.
- **Intervalo de portas do HDX Direct**: Define o intervalo de portas que o VDA usa para conexões de clientes externos.

Se necessário, a lista de servidores STUN usados pelo HDX Direct pode ser modificada editando o seguinte valor de registro:

- Chave: HKLM\SOFTWARE\Citrix\HDX-Direct
- Tipo de valor: REG_MULTI_SZ

- Nome do valor: STUNServers
- Dados: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

> **NOTA:**
>
> O HDX Direct para usuários externos está disponível apenas com EDT (UDP) como protocolo de transporte. Portanto, Transporte Adaptável deve ser habilitado.

## Considerações

A seguir estão as considerações para usar o HDX Direct:

- O HDX Direct para usuários externos está disponível apenas com EDT (UDP) como protocolo de transporte. Portanto, o **Transporte Adaptável** deve ser habilitado.
- Se você estiver usando o **HDX Insight**, observe que o uso do **HDX Direct** impede a coleta de dados do HDX Insight, pois a sessão não seria mais proxy através do NetScaler Gateway.
- Em ambientes com hosts de sessão multi-sessão, o HDX Direct exige que o logon do usuário seja concluído em um minuto. Se o tempo de logon exceder esse limite, o HDX Direct não será acionado e a sessão permanecerá conectada através do Gateway. Você pode aumentar o tempo limite do HDX Direct para suportar tempos de logon mais longos. Consulte Recursos do HDX gerenciados através do registro para obter detalhes.

## Como funciona

O HDX Direct permite que os clientes estabeleçam uma conexão direta com o host da sessão quando a comunicação direta estiver disponível. Quando as conexões diretas são feitas usando o HDX Direct, certificados autoassinados são usados para proteger a conexão direta com criptografia em nível de rede (TLS/DTLS).

### Usuários internos

O diagrama a seguir descreve a visão geral do processo de conexão HDX Direct para usuários internos.

Visão geral do HDX Direct(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-direct-overview.png)

1. O cliente estabelece uma sessão HDX através do Serviço de Gateway.

2. Após uma conexão bem-sucedida, o VDA envia ao cliente o FQDN da máquina VDA, uma lista de seus endereços IP e o certificado da máquina VDA via conexão HDX.
3. O cliente sonda os endereços IP para verificar se consegue alcançar o VDA diretamente.
4. Se o cliente conseguir alcançar o VDA diretamente com qualquer um dos endereços IP compartilhados, o cliente estabelece uma conexão direta com o VDA, protegida com (D)TLS usando um certificado que corresponde ao trocado na etapa (2).
5. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço de Gateway é encerrada.

> **Observação:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

#### Conexões diretas tradicionais

Ao usar Storefront, Workspace com Conexão Direta de Carga de Trabalho ou Workspace configurado para conectividade apenas interna, as conexões diretas são estabelecidas entre o cliente e o host da sessão sem a necessidade de rotear primeiro por um Gateway.

Nesses casos, o HDX Direct não é acionado, pois as conexões são inerentemente diretas. No entanto, se o HDX Direct estiver habilitado, essas conexões utilizarão os certificados HDX Direct para proteger as sessões.

### Usuários externos

O diagrama a seguir descreve a visão geral do processo de conexão HDX Direct para usuários externos:

Processo de conexão HDX Direct(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-direct-connection-process.png)

1. O cliente estabelece uma sessão HDX através do Serviço de Gateway.
2. Após uma conexão bem-sucedida, tanto o cliente quanto o VDA enviam uma solicitação STUN para descobrir seus endereços IP públicos e portas.

3. O servidor STUN responde ao cliente e ao VDA com seus endereços IP públicos e portas correspondentes.
4. Através da conexão HDX, o cliente e o VDA trocam seus endereços IP públicos e portas UDP, e o VDA envia seu certificado ao cliente.
5. O VDA envia pacotes UDP para o endereço IP público e porta UDP do cliente. O cliente envia pacotes UDP para o endereço IP público e porta UDP do VDA.
6. Ao receber uma mensagem do VDA, o cliente responde com uma solicitação de conexão segura.
7. Durante o handshake DTLS, o cliente verifica se o certificado corresponde ao certificado trocado na etapa (4). Após a validação, o cliente envia seu token de autorização. Uma conexão direta segura é agora estabelecida.
8. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço Gateway é encerrada.

> **Observação:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

## Compatibilidade NAT

Para estabelecer uma conexão direta entre um dispositivo de usuário externo e o host da sessão, o HDX™ Direct utiliza hole punching para travessia NAT e STUN para facilitar a troca do endereço IP público e mapeamentos de porta para o dispositivo cliente e o host da sessão. Isso é semelhante ao funcionamento de soluções VoIP, comunicações unificadas e P2P.

Desde que os firewalls e outros componentes de rede estejam configurados para permitir o tráfego UDP para as solicitações STUN e as sessões HDX, espera-se que o HDX Direct para usuários externos funcione. No entanto, existem certos cenários em que os tipos de NAT das redes do usuário e do host da sessão levam a uma combinação incompatível, fazendo com que o HDX Direct falhe.

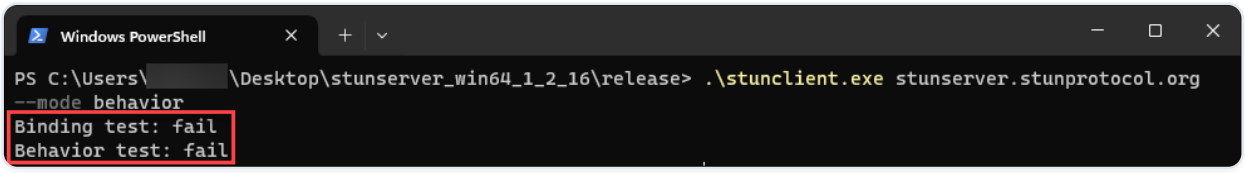
### Validações

Você pode validar o tipo e o filtro NAT no cliente e no host da sessão usando o utilitário cliente STUN do STUNTMAN:

1. Baixe o pacote apropriado para a plataforma de destino em stunprotocol.org e extraia o conteúdo.
2. Abra um prompt de terminal e navegar até o diretório onde o conteúdo foi extraído.
3. Execute o seguinte comando para realizar o teste de vinculação e comportamento NAT:
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. Se os testes de vinculação e comportamento forem bem-sucedidos, tanto o **teste de vinculação** quanto o **teste de comportamento** reportarão o sucesso e um comportamento NAT será especificado:

   Se os testes falharem, o **teste de vinculação** e/ou o **teste de comportamento** reportarão a falha.

5. Execute o seguinte comando para realizar o teste de vinculação e filtragem NAT:
   `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. Se os testes de vinculação e filtragem forem bem-sucedidos, tanto o **teste de vinculação** quanto o **teste de filtragem** reportarão o sucesso e um tipo de filtragem NAT será especificado:

   Se os testes falharem, o **teste de vinculação** e/ou o **teste de filtragem** reportarão a falha.

Após realizar os testes acima, verifique a tabela a seguir para determinar se o HDX Direct para usuários externos deve funcionar com base na combinação de comportamento e filtragem NAT:

| COMPORTAMENTO NAT DO CLIENTE | FILTRAGEM NAT DO CLIENTE | COMPORTAMENTO NAT DO HOST DE SESSÃO | FILTRAGEM NAT DO HOST DE SESSÃO | ESPERADO QUE FUNCIONE? |
|---|---|---|---|---|
| Mapeamento Independente de Endpoint | Qualquer | Mapeamento Independente de Endpoint | Qualquer | Sim |
| Mapeamento Independente de Endpoint | Filtragem Independente de Endpoint | Mapeamento Dependente de Endereço | Qualquer | Sim |
| Mapeamento Independente de Endpoint | Filtragem Dependente de Endereço | Mapeamento Dependente de Endereço | Qualquer | Não |
| Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço e Porta | Mapeamento Dependente de Endereço | Qualquer | Não |
| Mapeamento Independente de Ponto de Extremidade | Filtragem Independente de Ponto de Extremidade | Mapeamento Dependente de Endereço e Porta | Filtragem Independente de Ponto de Extremidade | Sim |
| Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço | Mapeamento Dependente de Endereço | Qualquer | Não |
| Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço e Porta | Mapeamento Dependente de Endereço | Qualquer | Não |
| Mapeamento Dependente de Endereço | Qualquer | Mapeamento Independente de Ponto de Extremidade | Filtragem Independente de Ponto de Extremidade | Sim |

| COMPORTAMENTO NAT DO CLIENTE | FILTRAGEM NAT DO CLIENTE | COMPORTAMENTO NAT DO HOST DE SESSÃO | FILTRAGEM NAT DO HOST DE SESSÃO | ESPERADO QUE FUNCIONE? |
|---|---|---|---|---|
| Mapeamento Dependente de Endereço | Qualquer | Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço | Não |
| Mapeamento Dependente de Endereço | Qualquer | Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço e Porta | Não |
| Mapeamento Dependente de Endereço | Qualquer | Mapeamento Dependente de Endereço | Qualquer | Não |
| Mapeamento Dependente de Endereço | Qualquer | Mapeamento Dependente de Endereço e Porta | Qualquer | Não |
| Mapeamento Dependente de Endereço e Porta | Qualquer | Mapeamento Independente de Endpoint | Filtragem Independente de Endpoint | Sim |
| Mapeamento Dependente de Endereço e Porta | Qualquer | Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço | Não |
| Mapeamento Dependente de Endereço e Porta | Qualquer | Mapeamento Independente de Ponto de Extremidade | Filtragem Dependente de Endereço e Porta | Não |
| Mapeamento Dependente de Endereço e Porta | Qualquer | Mapeamento Dependente de Endereço | Qualquer | Não |

| COMPORTAMENTO NAT DO CLIENTE | FILTRAGEM NAT DO CLIENTE | COMPORTAMENTO NAT DO HOST DE SESSÃO | FILTRAGEM NAT DO HOST DE SESSÃO | ESPERADO QUE FUNCIONE? |
|---|---|---|---|---|
| Mapeamento Dependente de Endereço e Porta | Qualquer | Mapeamento Dependente de Endereço e Porta | Qualquer | Não |
| Falha | Qualquer | Qualquer | Qualquer | Não |
| Qualquer | Qualquer | Falha | Qualquer | Não |
| Falha | Qualquer | Falha | Qualquer | Não |

## Solução de problemas

Para confirmar que o **HDX Direct** estabeleceu com sucesso uma conexão direta, você pode usar o utilitário `CtxSession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se a conexão **HDX Direct** for estabelecida com sucesso, o **HDX Direct Status** será `Connected`.

```
PS C:\Users\                    > ctxsession -v

Session Id  1:
Transport Protocols:    UDP -> DTLS -> CGP -> ICA
      Local Address:                        :55000
     Remote Address:                        :60410
     Client Address:                        :63274
  Security Protocol:    DTLS 1.2
    Security Cipher:    256 bit AES
    Cipher Strength:    256 bits
     ICA Encryption:    Transport Only
 Rendezvous Version:    None
   HDX Direct State:    Connected - External
    Reducer Version:    4.0

EDT Reliable Statistics:
    Bandwidth 301.904 Mbps,  RTT 57.690 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 35.164 ms,  EDT MTU: 1480

ICA Statistics:
     SentBandwidth (bps)      =          0
     HDX Latency              =         63
     IcaBufferLength          =       1436
```

Você também pode consultar os logs de eventos do host da sessão para obter informações sobre se a conexão HDX™ Direct foi estabelecida com sucesso ou falhou. Consulte a seção **Logs de Eventos** para obter detalhes.

> Nota:
>
> Dependendo do ambiente e do número de endereços IP disponíveis para os hosts da sessão, pode levar até 5 minutos para que a conexão HDX Direct seja estabelecida.

### Quando o HDX Direct falha ao estabelecer uma conexão direta

Se o HDX Direct estiver falhando ao estabelecer uma conexão direta, revise as seguintes etapas:

1. Certifique-se de que a versão do VDA e a versão do aplicativo Workspace em uso suportam o recurso de acordo com os requisitos do sistema.
2. Confirme se você tem uma política aplicada ao VDA que habilita o HDX Direct e que não há outras políticas com prioridade mais alta desabilitando o recurso.
3. Confirme se você tem uma política aplicada ao VDA que define o modo HDX Direct desejado e que não há outras políticas com prioridade mais alta sobrescrevendo a configuração.
4. Certifique-se de que o Serviço Citrix ClxMtp esteja em execução no host da sessão.
5. Certifique-se de que o Serviço Citrix Certificate Manager esteja em execução no host da sessão. Se não estiver em execução, tente iniciá-lo manualmente. O serviço para automaticamente se o HDX Direct estiver desabilitado.
6. Verifique se o host da sessão possui seu certificado de CA Raiz autoassinado:
    a. Emitido para: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
7. Verifique se o host da sessão possui seu certificado de servidor autoassinado:
    a. Emitido para: `<host FQDN>` (Por exemplo, FTLW11-001.ctxlab.net)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
8. Se os certificados estiverem ausentes, entre em contato com o Suporte Técnico da Citrix.
9. Se os certificados estiverem presentes:
    a. Pare o Serviço de Gerenciamento de Certificados Citrix no host da sessão.
    b. Exclua ambos o certificado de CA Raiz autoassinado e o certificado de servidor autoassinado.
    c. Inicie o Serviço de Gerenciamento de Certificados Citrix no host da sessão. O serviço cria novos certificados assim que é iniciado.
10. Para usuários internos:
    a. Certifique-se de que o firewall do host da sessão não esteja bloqueando o tráfego de entrada nas portas UDP 443 ou TCP 443, para HDX sobre EDT e HDX sobre TCP, respectivamente.

b. Certifique-se de que seu firewall de rede não esteja bloqueando o tráfego nas portas UDP 443 e TCP 443 entre a rede dos seus clientes e a rede dos hosts da sessão.

11. Para usuários externos:

a. Verifique o tipo de NAT para o cliente e o host da sessão e certifique-se de que a combinação deve funcionar. Consulte a seção Compatibilidade de NAT para obter detalhes.

b. Se o teste de NAT falhar no cliente ou no host da sessão:

i. Se houver um firewall em execução no sistema, certifique-se de que ele não esteja bloqueando o tráfego de saída na porta UDP 3478.

ii. Certifique-se de que seus firewalls de rede não estejam bloqueando o tráfego de saída na porta UDP 3478.

iii. Certifique-se de que os firewalls não estejam bloqueando a resposta do servidor STUN.

c. Certifique-se de que seus firewalls de rede tenham as regras apropriadas configuradas para permitir todo o tráfego necessário. Consulte a seção Requisitos de Rede para obter detalhes.

d. Se você alterar o intervalo de portas padrão usando a configuração de política de intervalo de portas HDX Direct, certifique-se de que suas regras de firewall estejam definidas para o intervalo de portas personalizado.

### Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA:

| LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operacional | 1 | HDX Direct | Informação | Conexão HDX Direct para o usuário interno `<username>` estabelecida. |
| Logs de Aplicativos e Serviços > Citrix- | 2 | HDX Direct | Informação | Conexão HDX Direct para usuário externo |

| LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| HostCore-HDX Direct/ Operacional | | | | `<username>` estabelecida. |
| Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operacional | 3 | HDX Direct | Informações | Conexão HDX Direct para o usuário `<username>` falhou. |

### Problemas conhecidos

O HDX Direct pode parar de funcionar após a realização de um upgrade in-loco do VDA em uma máquina que já tenha o **HDX Direct** habilitado. Para resolver o problema, conclua as seguintes etapas:

1. Pare o Serviço de Gerenciamento de Certificados Citrix no host da sessão.
2. Exclua o certificado autoassinado da CA Raiz e o certificado autoassinado do servidor.
3. Abra o registro.
4. Exclua a chave `HKLM\Software\Citrix\HDX-Direct`.
5. Vá para `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Defina o valor **SSLEnabled** como `0`.
7. Exclua o conteúdo do valor **SSLThumbprint**.
8. Inicie o **Serviço de Gerenciamento de Certificados Citrix**.

## HDX Seguro™

O HDX Seguro é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que quaisquer elementos de rede no caminho do tráfego inspecionem o tráfego HDX. Isso é feito fornecendo Criptografia de Ponta a Ponta (E2EE) verdadeira no nível do aplicativo entre o aplicativo Citrix Workspace™ (cliente) e o VDA (host de sessão) usando criptografia AES-256-GCM.

## Requisitos do sistema

A lista a seguir descreve os requisitos do sistema para usar o HDX Seguro.

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 ou posterior
- Host de sessão
  - Sistema operacional
    - Windows 10 22H2
    - Windows 11 22H2 ou posterior
    - Windows Server 2019 ou posterior
  - Virtual Delivery Agent (VDA)
    - Windows: versão 2503 ou posterior
    - Linux: versão 2407 ou posterior
- Aplicativo Workspace
  - Windows: versão 2503 ou posterior
  - Linux: versão 2408 ou posterior
  - Mac: versão 2409 ou posterior
  - Chrome OS: versão 2409 ou posterior
  - HTML5: versão 2408 ou posterior
  - Android: versão 2503 ou posterior
  - iOS: versão 2503 ou posterior
- Camada de acesso
  - Citrix Workspace
  - Citrix StoreFront™ 2402 ou posterior

**NOTA:**

> O suporte com Citrix Virtual Apps and Desktops™ 2402 LTSR está disponível com **CU3** ou posterior.

> Para obter detalhes sobre a configuração do Secure HDX com Linux VDA, consulte a documentação do Linux VDA.

## Configuração

O Secure HDX está desativado por padrão. Você pode configurar esse recurso usando a configuração Secure HDX na política do Citrix:

**Secure HDX**: Define se o recurso deve ser ativado ou desativado.

> **IMPORTANTE:**

> Se você tiver o Secure ICA® ativado nos grupos de entrega nos quais deseja ativar o Secure HDX, você deve primeiro desativar o Secure ICA (Editar grupo de entrega > Configurações do usuário).

## Considerações

A seguir estão as considerações para usar o Secure HDX:

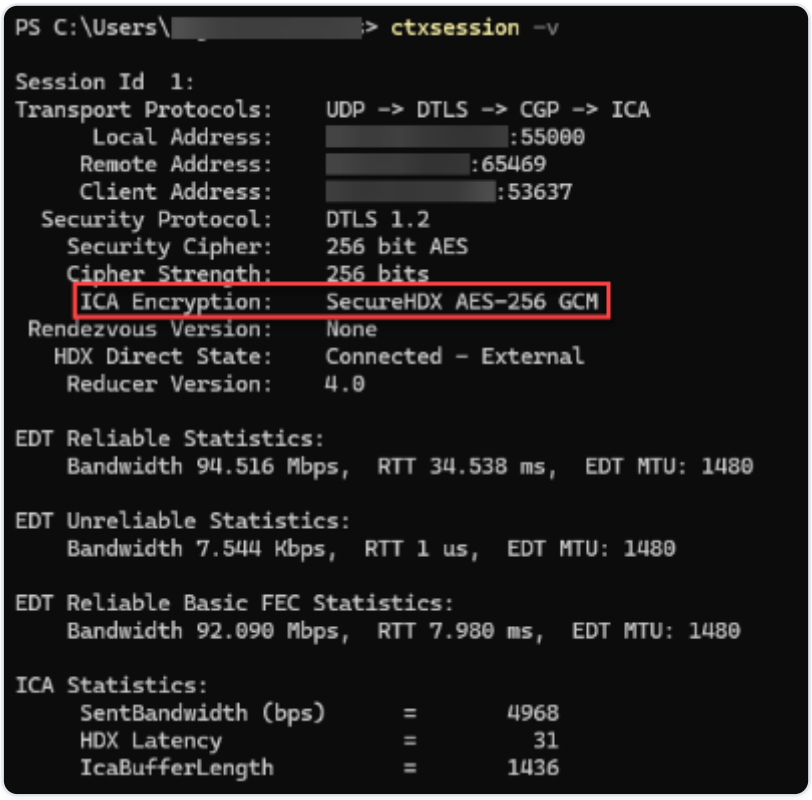
- Se um usuário tentar se conectar a um host de sessão com o Secure HDX ativado usando um cliente que não oferece suporte ao recurso, a conexão será negada.
- Apenas Service Continuity para cargas de trabalho sem conector é suportado com o Secure HDX. Se você estiver usando a versão padrão do Service Continuity, não conseguirá se conectar a nenhum host de sessão que tenha o Secure HDX ativado se houver uma interrupção do serviço de nuvem.
- 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, será necessário fazer upgrade para o Citrix Virtual Apps and Desktops 2503 ou mais recente e habilitar Telemetria de rede.
- Se você usa o SmartControl, observe que o uso do Secure HDX impede o funcionamento do SmartControl, pois o NetScaler não consegue inspecionar o tráfego HDX criptografado. Se você precisar usar o SmartControl, será necessário fazer upgrade para o Citrix Virtual Apps and Desktops 2503 ou mais recente e habilitar Telemetria de rede.

- O ICA Multi-Stream não é suportado quando o Secure HDX está ativado.
- Se você usar soluções de terceiros que dependem da inspeção do tráfego HDX, elas não funcionarão mais se você ativar o Secure HDX, pois o tráfego HDX é criptografado.

## Solução de problemas

Para confirmar que o Secure HDX está ativo, você pode usar o utilitário `ctxsession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, abra um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se o Secure HDX estiver em uso, a Criptografia ICA exibirá `SecureHDX AES-256 GCM`.




### Quando o Secure HDX não é ativado na sessão

- Certifique-se de que a versão do VDA em uso suporte o recurso de acordo com os requisitos do sistema.
- Confirme se você tem uma política aplicada ao VDA que habilita o Secure HDX e que não há outras políticas com prioridade mais alta desativando o recurso.
- Se o host da sessão já estava em execução quando você configurou o Secure HDX, reinicie a máquina para garantir que as alterações entrem em vigor.

# Lista de permissões de canais virtuais

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas os canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

## Configuração

A lista de permissões de canal virtual é habilitada por padrão. Você pode configurar esse recurso usando as seguintes configurações na política Citrix:

- **Lista de permissões de canais virtuais**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.
- **Limitação de log da lista de permissões de canais virtuais**: define o período de limitação para o registro de eventos da lista de permissões de canais virtuais.
- **Registro em log da lista de permissões de canais virtuais**: define o nível de registro em log para a lista de permissões de canais virtuais.

## Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando a configuração de política da lista de permissões de canais virtuais. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

### Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

### Para vários processos

Se houver vários processos, adicione a seguinte entrada à lista:

`CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe`

### Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar caracteres curinga nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O caractere curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`
- Todos os caminhos devem ser locais.

> **Nota:**

- Caminhos de rede não são permitidos.
- O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
- O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

### Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

**Nota:**

Variáveis de ambiente de usuário não são suportadas.

O suporte a variáveis de ambiente está disponível a partir do Citrix Virtual Apps and Desktops versão 2209.

## Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política de lista de permissões de canais virtuais para o canal virtual e o processo identificados.
5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

## Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- Pacote de Otimização HDX RealTime para Skype for Business

### Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`
- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.

- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### Pacote de Otimização HDX RealTime para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Solução de problemas

Se o seu canal virtual personalizado não abrir, revise as seguintes etapas:

1. Certifique-se de que você está usando a versão correta do VDA.
2. Confirme se você tem uma política aplicada ao VDA com o canal virtual personalizado na lista de permissões de canais virtuais e que não há outras políticas com prioridade mais alta sobrescrevendo essa configuração.
3. Verifique o log de eventos no VDA e confirme se o nome do canal virtual relatado corresponde ao definido na lista de permissões.
    a. Se você tiver vários processos, certifique-se de que eles estejam definidos corretamente, conforme descrito em Adicionar canais virtuais à lista de permissões.
    b. Se você estiver usando curingas no caminho do processo definido, certifique-se de estar seguindo as diretrizes para Usar curingas.
    c. Se você estiver usando variáveis de ambiente no caminho do processo definido, certifique-se de estar seguindo as diretrizes em Usar variáveis de ambiente do sistema.

### Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA.

#### VDA de sessão única

Os seguintes eventos são registrados no log de eventos da máquina VDA de sessão única:

| NOME DO LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| Sistema | 2001 | `Picadd` | Informação | O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>` |
| Sistema | 2002 | `Picadd` | Aviso | O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>` |
| Sistema | 2003 | `Picadd` | Informação | `<username>` abriu o canal virtual personalizado `<vcName>` |
| Sistema | 2004 | `Picadd` | Aviso | `<username>` tentou abrir o canal virtual personalizado `<vcName>` |
| Sistema | 2005 | `Picadd` | Erro | O caminho fornecido na política `<pathInPolicy>` não pode ser resolvido para o caminho do processo |
| Sistema | 2007 | `Picadd` | Informação | O caminho do processo carregado é |

| NOME DO LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| | | | | `<processPath>` |
| Sistema | 2008 | `Picadd` | Erro | A variável de ambiente `<varName>` no caminho da política VC não foi encontrada |

### VDA multissessão

Os seguintes eventos são registrados no log de eventos da máquina VDA multissessão:

| NOME DO LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| Sistema | 13 | `Rpm` | Informação | O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>` |
| Sistema | 14 | `Rpm` | Aviso | O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>` |
| Sistema | 15 | `Rpm` | Informação | `<username>` abriu o canal virtual personalizado `<vcName>` |
| Sistema | 16 | `Rpm` | Aviso | `<username>` tentou abrir o |

| NOME DO LOG | ID | ORIGEM | NÍVEL | DESCRIÇÃO |
|---|---|---|---|---|
| | | | | canal virtual personalizado `<vcName>` |
| Sistema | 17 | `Rpm` | Erro | O caminho fornecido na política `<pathInPolicy>` não pode ser resolvido para o caminho do processo |
| Sistema | 18 | `Rpm` | Informação | O caminho do processo carregado é `<processPath>` |
| Sistema | 19 | `Rpm` | Erro | Variável de ambiente `<varName>` no caminho da política VC não encontrada |

## Canais virtuais de terceiros conhecidos

A seguir estão soluções de terceiros conhecidas que usam canais virtuais Citrix® personalizados. Esta lista não inclui todas as soluções que usam um canal virtual Citrix personalizado.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- deviceTrust
- Epic Warp Drive
- Epic Slingshot

- Imprivata OneSign
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Reuniões Zoom para VDI
- Ultima IA-Connect

Para obter detalhes sobre como adicionar os canais virtuais associados à lista de permissões, entre em contato com os fornecedores das soluções. Alternativamente, siga as etapas descritas na seção Obtaining virtual channel names and processes.

# Dispositivos

O HDX™ oferece uma experiência de usuário de alta definição em qualquer dispositivo, em qualquer local. Os artigos na seção Dispositivos descrevem estes dispositivos:

- Digitalização
- Dispositivo USB genérico
- Mapeamento de Unidade Cliente
- Dispositivos móveis e de tela sensível ao toque
- Dispositivos seriais
- Teclados especiais
- Webcams

## Dispositivo USB otimizado vs. genérico

Um dispositivo USB otimizado é aquele para o qual o aplicativo Citrix Workspace™ tem suporte específico. Por exemplo, a capacidade de redirecionar webcams usando o canal virtual HDX Multimedia. Um dispositivo genérico é um dispositivo USB para o qual não há suporte específico no aplicativo Citrix Workspace.

Por padrão, o redirecionamento USB genérico não pode redirecionar dispositivos USB com suporte a canal virtual otimizado, a menos que sejam colocados no modo Genérico.

Em geral, você obtém melhor desempenho para dispositivos USB no modo Otimizado do que no modo Genérico. No entanto, há casos em que um dispositivo USB não possui funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos seus recursos.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados por políticas Citrix®. As principais diferenças são:

Se o redirecionamento USB genérico e as políticas de mapeamento de unidade cliente estiverem habilitados e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidade cliente.

Quando estas condições são verdadeiras, o dispositivo de armazenamento em massa é redirecionado usando o redirecionamento USB genérico:

- Tanto o redirecionamento USB genérico quanto as políticas de mapeamento de unidade do cliente estão ativados.
- Um dispositivo está configurado para redirecionamento automático.
- Um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão.

Para obter mais informações, consulte `<http://support.citrix.com/article/CTX123015>`.

| RECURSO | MAPEAMENTO DE UNIDADE DO CLIENTE | REDIRECIONAMENTO USB GENÉRICO |
|---|---|---|
| Ativado por padrão | Sim | Não |
| Acesso somente leitura configurável | Sim | Não |
| Acesso a dispositivo criptografado | Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado na sessão virtual. | Somente Citrix Virtual Desktops™ |

# Digitalização

O scanner é um dispositivo que digitaliza opticamente imagens, texto impresso, caligrafia ou um objeto e os converte em uma imagem digital.

Se você estiver usando um scanner e seu computador estiver executando o Windows, há uma boa chance de você estar usando o driver de scanner WIA. Este driver é responsável pela comunicação entre seu computador e o scanner.

- **Windows Image Acquisition** (WIA) é o modelo de driver e a interface de programação de aplicativos (API) da Microsoft que permite que o software se comunique com hardware de imagem, como scanners.
- **TWAIN** (Windows e Mac) é outro protocolo, um protocolo de digitalização que conecta scanners e aplicativos, fornecendo uma interface padrão. O TWAIN permite que os aplicativos adquiram imagens de dispositivos compatíveis com TWAIN (scanners, câmeras digitais, etc.).

# Redirecionamento TWAIN

## Introdução

TWAIN é um protocolo de digitalização usado para vincular software de imagem a scanners ou câmeras digitais.

### Como o TWAIN funciona

- Digitalize seus documentos usando qualquer um dos aplicativos de 32 bits em sua sessão Citrix®.

> **Nota:**
>
> Use um scanner conectado localmente e compatível com TWAIN para digitalizar os documentos.

- O módulo de digitalização Citrix redireciona a solicitação TWAIN para o scanner do cliente.
- Assim que a digitalização é concluída, o host da sessão é notificado.

## Requisitos

### Plano de Controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

### Host da Sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11
  - Windows Server 2022 ou posterior
- VDA
  - Versão 1912 ou posterior
- Aplicativo
  - Aplicativo de 32 bits

### Dispositivo Cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11
- Aplicativo Workspace
  - Windows: versão 1912 ou posterior
- Scanner
  - Scanner compatível com TWAIN

## Configuração

- Instale os drivers TWAIN no endpoint do cliente.
- Configure dispositivos ou aplicativos para selecionar o protocolo de digitalização necessário se eles suportarem TWAIN e WIA.
- Conecte o scanner ao endpoint do cliente localmente (via USB).
- Redirecione os dispositivos TWAIN para a sessão via redirecionamento USB, se necessário.

> **Nota:**
>
> Dispositivos TWAIN não funcionam bem com o redirecionamento USB, resultando em baixa qualidade de digitalização.

### Configurações de Política

Configurações de política para configurar o redirecionamento TWAIN e melhorar a digitalização.

- **Redirecionamento de dispositivo TWAIN do cliente:** para habilitar ou desabilitar o redirecionamento TWAIN.

> **Nota:**
>
> Por padrão, o redirecionamento TWAIN está habilitado.

- **Nível de compactação TWAIN:** para definir os níveis de compactação para imagens do cliente para o host.

Para mais detalhes, consulte configurações de política de dispositivos TWAIN.

### Solução de problemas

Experimente o TWAIN com o aplicativo de teste público Twacker, que pode ser baixado neste URL.

Siga as etapas para validar o TWAIN em uma sessão de área de trabalho publicada:

1. Instale **Twacker** no VDA.
2. Inicie **Twacker** (versão de 32 bits).
3. Clique em **Arquivo > Selecionar Origem** e selecione seu scanner na lista.
4. Clique em **Arquivo > Adquirir**.
5. Clique no **botão Digitalizar** para testar seu scanner.

Se **Twacker** conseguir digitalizar com sucesso, isso confirma que a configuração do **Citrix Virtual Apps and Desktops** é:

- Configurada para redirecionamento USB
- Usando dispositivos TWAIN
- Atendendo a todos os requisitos do dispositivo cliente local

Se você ainda tiver problemas de digitalização em um aplicativo específico, então é provável que seja um problema de software.

## Dispositivos WIA

### Requisitos

- O scanner deve ser compatível com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, via USB).
- Certifique-se de que o scanner esteja usando o serviço local do Windows Image Acquisition e não o driver TWAIN.

- Certifique-se de que nenhuma política seja aplicada à conta de usuário usada para o teste, e que esteja limitando a largura de banda dentro da sessão ICA®. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

**Lista de permissão de aplicativos de aquisição de imagem do Windows**

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento de scanner do Windows Image Acquisition. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém o Windows Image Acquisition. Por padrão, nenhum aplicativo tem acesso ao Windows Image Acquisition.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração Lista de permissões de aplicativos do Windows Image Acquisition na lista de recursos gerenciados através do registro.

Para obter informações sobre as configurações de política, consulte Configurações de política de dispositivos WIA.

# Dispositivos USB genéricos

## Introdução

O recurso de redirecionamento USB genérico permite o redirecionamento de dispositivos USB de máquinas cliente para sessões HDX™, dando aos usuários finais a capacidade de interagir com uma ampla seleção de dispositivos USB genéricos em sua sessão HDX. Isso é útil em cenários onde os usuários precisam usar dispositivos especializados que não possuem suporte otimizado ou onde é inadequado.

> **Nota:** Dispositivos USB não otimizados para suporte a canal virtual recorrerão ao canal virtual USB Genérico usando redirecionamento USB bruto.

## Como funciona?

O redirecionamento USB genérico funciona em um nível baixo e redireciona mensagens de solicitação e resposta USB entre máquinas cliente e o desktop virtual XenDesktop®.

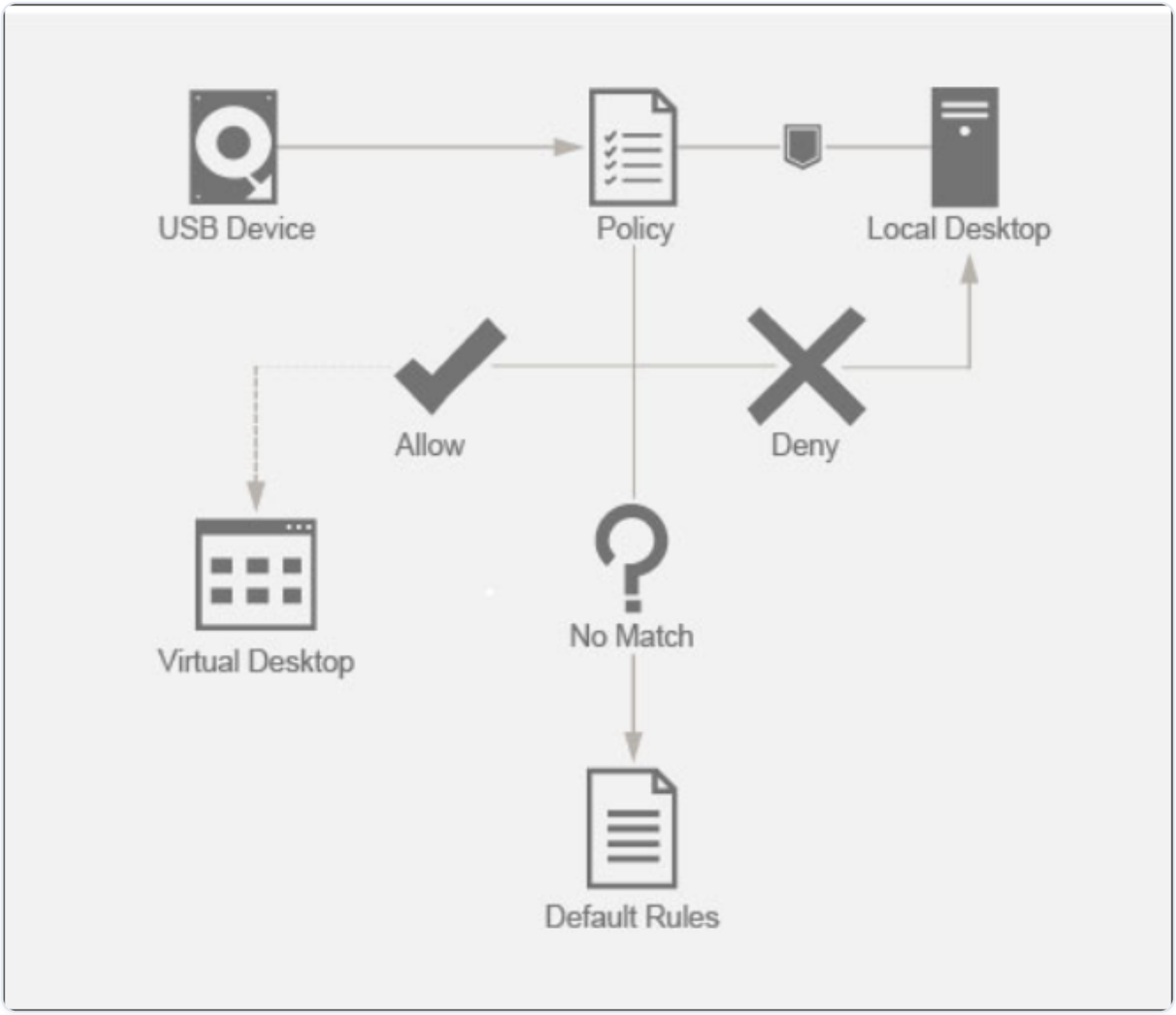
Ele evita a exigência de drivers de dispositivo compatíveis na máquina cliente e espera-se que o driver seja suportado apenas no desktop virtual. As regras de política de redirecionamento USB seguem uma certa ordem de precedência que permite que políticas do lado do cliente e regras padrão sejam respeitadas depois que as regras de política do DDC forem avaliadas e aplicadas.

Isso permite que os administradores da Citrix evitem que quaisquer dispositivos não autorizados/falsificados sejam redirecionados para dentro de uma sessão.

Além disso, o registro de eventos de dispositivos não autorizados que tentam acessar a sessão remota pode ser auditado e sinalizado, e os administradores podem tomar medidas adicionais para evitar a exfiltração de dados.

Quando um usuário conecta um dispositivo USB, o host da sessão o verifica consecutivamente contra cada regra de política até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva.

- Se a primeira correspondência for uma regra de Permissão, o dispositivo é redirecionado para o desktop virtual.
- Se a primeira correspondência for uma regra de Negação, o dispositivo não é redirecionado para a sessão e só está disponível para uso no dispositivo do usuário local. Se nenhuma correspondência for encontrada, as regras padrão são usadas.



# Configuração

O redirecionamento USB está desabilitado por padrão. Você pode configurar o redirecionamento USB genérico usando as seguintes configurações na política Citrix®:

- **Redirecionamento de dispositivo USB do cliente**: para habilitar ou desabilitar o redirecionamento USB
- **Regras de redirecionamento de dispositivo USB do cliente**: para especificar uma ação de dispositivo específica, ou seja, para permitir ou negar acesso a um dispositivo específico
- **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**: para especificar regras para filtrar, dividir e conectar automaticamente dispositivos USB
- **Regras de otimização de dispositivo USB do cliente**: para desabilitar a otimização ou alterar o modo de otimização
- **Permitir que dispositivos USB existentes sejam conectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB existentes que estão conectados a um endpoint cliente no início de uma sessão HDX™
- **Permitir que dispositivos USB recém-chegados sejam detectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB que são conectados a um endpoint cliente durante uma sessão HDX

Consulte Configurações de Política USB para obter mais detalhes.

## Como configurar o redirecionamento USB

Por padrão, a configuração de redirecionamento USB está desabilitada. Para usá-lo, a política de redirecionamento USB e as regras de redirecionamento específicas devem ser habilitadas e configuradas no DDC.

> **Observação:**
>
> Se você estiver usando componentes anteriores à versão 2212 ou estiver usando o Workspace App para Linux/Mac, consulte Configuração de Redirecionamento USB Legado para obter detalhes sobre como configurar o redirecionamento USB.

### Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.

3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

### Criação de Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em relação a cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de **Permitir**, o dispositivo correspondente tem permissão para ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de **Negar**, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

#### REGRAS DE DISPOSITIVO

Assim como nos dispositivos USB regulares, as regras de dispositivo definidas na política ou na configuração do aplicativo cliente Citrix Workspace™ no ponto de extremidade selecionam os dispositivos para encaminhamento. O aplicativo Citrix Workspace™ usa essas regras para decidir quais dispositivos USB permitir ou impedir de serem encaminhados para a sessão remota.

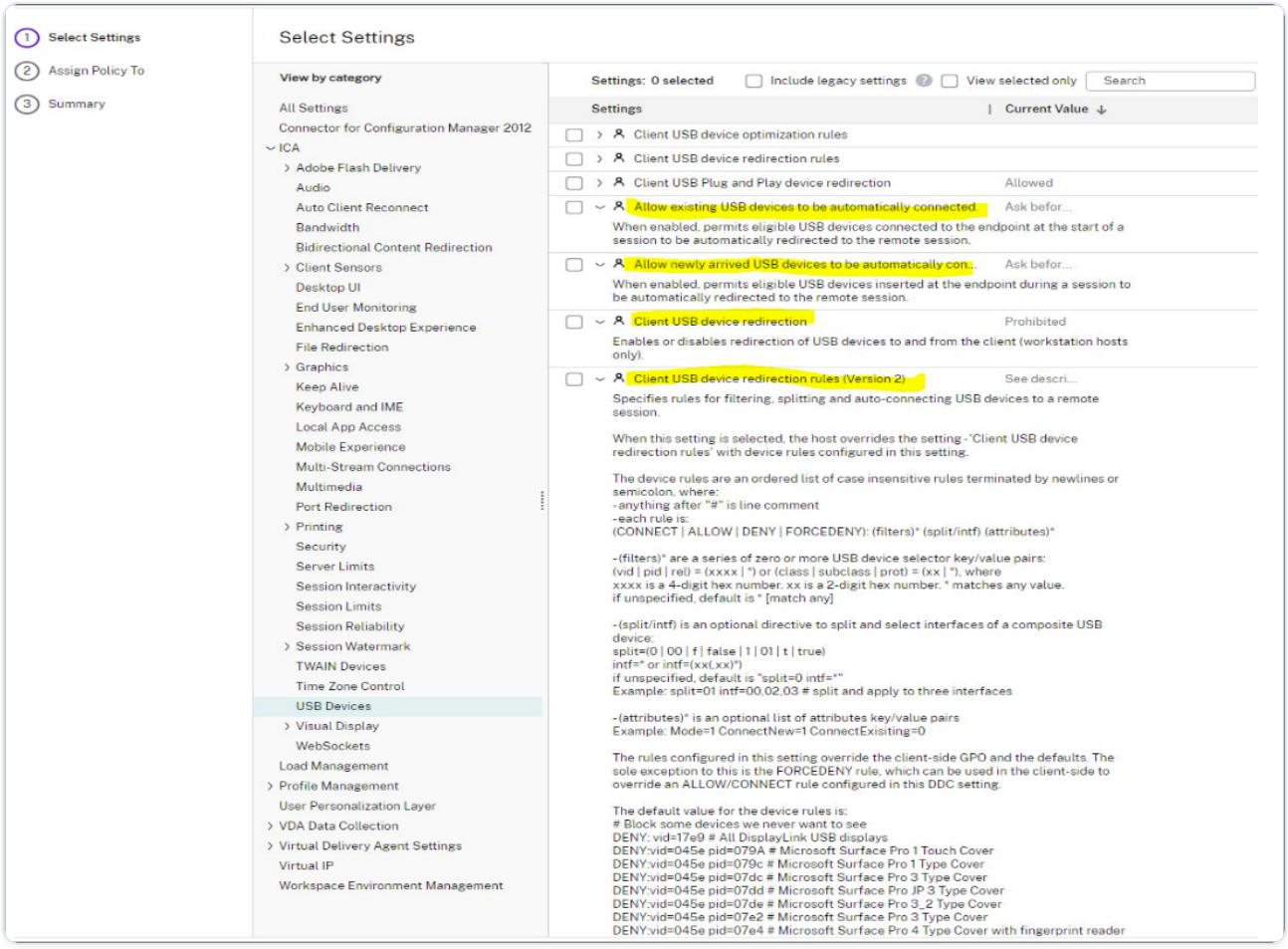
Cada regra consiste em uma palavra-chave de ação (**Permitir, Conectar ou Negar**), dois pontos (:) e zero ou mais parâmetros de filtro que correspondem a dispositivos reais no subsistema USB dos pontos de extremidade. Esses parâmetros de filtro correspondem aos metadados do descritor de dispositivo USB usados por cada dispositivo USB para se identificar.

As regras de dispositivo são texto simples, com cada regra em uma única linha e um comentário opcional após um caractere #. As regras são correspondidas de cima para baixo (ordem de prioridade decrescente). A primeira regra que corresponde ao dispositivo ou interface filho é aplicada. As regras subsequentes que selecionam o mesmo dispositivo ou interface são ignoradas.

**Exemplo:** ALLOW VID=1050 PID=0421 #Device1 **Exemplo:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

| PALAVRA-CHAVE | DESCRIÇÃO |
|---|---|
| CONNECT | Use esta palavra-chave para permitir que os dispositivos sejam redirecionados através do canal virtual USB, bem como para permitir que sejam redirecionados automaticamente durante o início da sessão e após a inserção. |

| PALAVRA-CHAVE | DESCRIÇÃO |
| --- | --- |
| ALLOW | Use esta palavra-chave para permitir que os dispositivos sejam redirecionados através do canal virtual USB |
| DENY | Use esta palavra-chave para negar que os dispositivos sejam redirecionados através do canal virtual USB |




**Configurando a política no DDC**:

1. Abra **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar.

   Por Exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Armazenamento em Massa

> **Observação:**
>
> Se um administrador Citrix marcar **Usar valor padrão** e clicar em **Salvar**, as regras padrão podem ser encontradas no seguinte registro no VDA.
>
> **Cuidado!**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Observação:**
>
> As políticas ainda podem ser definidas no dispositivo cliente usando regras de dispositivo de política de grupo, mas isso não é mais necessário nas versões mais recentes do CVAD e CWA.
>
> Para configuração legada de dispositivos USB, consulte Configuração de Redirecionamento USB Legado.

**Configurar redirecionamento automático de dispositivos USB (Opcional)**

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use DeviceRules no endpoint do cliente ou na política do DDC. Esta política pode ser definida no DDC, no cliente usando um GPO, usando as Preferências do Citrix Workspace ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

**Configurando a política no DDC:**

Existem duas políticas no DDC que podem ser configuradas para permitir o redirecionamento automático de dispositivos USB-

- Permitir que dispositivos USB existentes sejam conectados automaticamente
- Permitir que dispositivos USB recém-chegados sejam conectados automaticamente

a. Abra **Citrix Web Studio policies** e clique na guia **Policies**.

b. Clique em **Create Policy** e expanda as **ICA > USB Devices policies**.

c. Edite a configuração **Allow** existing USB devices to be automatically connected.

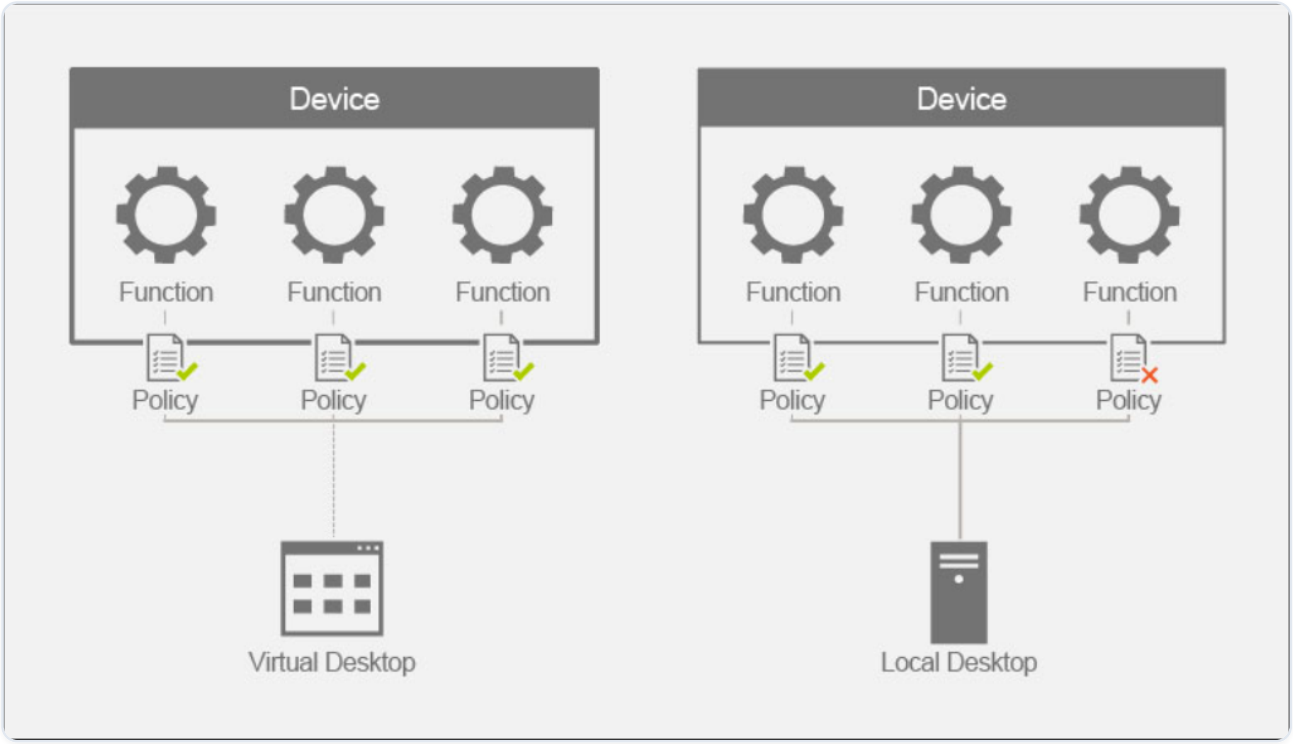
d. Desmarque a caixa de seleção **Use default value** e selecione **Automatically redirect available USB devices** no menu suspenso e clique em **Save**.

e. Edite a configuração **Allow** newly arrived USB devices to be automatically connected.

f. Desmarque a caixa de seleção **Use default value** e selecione **Automatically redirect available USB devices** no menu suspenso e clique em **Save**.

## Dispositivos Compostos e Divisão de Dispositivos

Um dispositivo USB composto é um único dispositivo que age como múltiplos dispositivos USB independentes conectados a um computador. Ele possui um único conector USB, mas pode expor múltiplas interfaces ao computador, cada uma com seu próprio conjunto de funcionalidades. Quando um usuário conecta um dispositivo USB composto, o dispositivo host verifica todas as funções (interfaces) em relação a cada regra de política. Se a primeira correspondência para qualquer função (interface) for uma regra de Negação, a regra é considerada definitiva para o dispositivo composto e o dispositivo é negado. Se a primeira correspondência para uma função (interface) for uma regra de Permissão, o dispositivo host continua a corresponder as regras à próxima função (interface). O dispositivo composto é permitido se nenhuma função (interface) for negada por uma regra de política. Se a correspondência definitiva para o dispositivo composto for uma Regra de Negação, o dispositivo estará disponível apenas para o desktop local; caso contrário, o dispositivo é redirecionado para o desktop virtual. Se nenhuma correspondência for encontrada, as regras padrão são usadas.




Podemos dividir o dispositivo composto usando as regras apropriadas na política de regras de redirecionamento de dispositivo (Versão 2) para permitir apenas funcionalidades específicas de um dispositivo composto. Por exemplo, podemos querer usar apenas as funções HID de uma chave FIDO2, mas não a funcionalidade de smartcard. Nesse caso, definiríamos as regras conforme ilustrado abaixo:

1. Conectar: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da Yubikey série 5.
2. Negar: VID=1050 PID=0407 split=01 intf=02 # Função de cartão inteligente da Yubikey série 5 bloqueada.

> **Dica:**
>
> Ao criar novas regras de política, consulte os Códigos de Classe USB, disponíveis no site da USB.

### Configurando uma mesa digitalizadora de assinatura

1. Instale o driver de dispositivo apropriado no host VDA.
2. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** em **Citrix Web Studio™**.

3. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Defina as informações de **VID** e **PID** para a mesa digitalizadora de assinatura que precisa ser redirecionada e clique em **Salvar**. Por exemplo: **Conectar**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. Edite a configuração de política **Regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo juntamente com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=06A8 PID=0057 class=03 #Dispositivo de entrada operando em modo de captura
5. Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
7. Edite a configuração da política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, os lançamentos de sessão subsequentes terão o dispositivo redirecionado automaticamente e não exigirão nenhuma ação adicional do usuário final.

> **Nota:**
>
> Substitua o VID e o PID pelos VID e PID reais do dispositivo a ser redirecionado.

### Configurando o teclado Bloomberg usando o redirecionamento USB

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Os teclados Bloomberg 5 são definidos por padrão na configuração de política **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)** e nenhuma ação administrativa adicional é necessária.

3. Edite a configuração da política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração da política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, as chaves Bloomberg serão apresentadas automaticamente 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 chaves FIDO2 em suas sessões HDX. No entanto, pode haver situações em que você deve redirecionar chaves FIDO2 usando o redirecionamento USB. Isso inclui cenários em que o redirecionamento FIDO2 não está disponível porque o recurso não é compatível com o cliente, o VDA ou o sistema operacional (por exemplo, Windows Server 2016).

Também pode haver situações em que a chave tem vários modos ativados, mas você só quer permitir um subconjunto deles em suas sessões HDX. Por exemplo, você pode querer permitir FIDO2 e OTP, mas bloquear o cartão inteligente.

As etapas a seguir ilustram como você pode configurar uma chave FIDO2 usando o redirecionamento USB (Yubikey vid=1050, pid=0407).

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**.
    a. Defina as informações de **VID** e **PID**, bem como a configuração de divisão do dispositivo para que a chave FIDO2 seja redirecionada na sessão e clique em **Salvar**.
    b. **Conectar**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da série 5 da Yubikey.
    c. **Negar**: VID=1050 PID=0407 split=01 intf=02 # Função de cartão inteligente da série 5 da Yubikey bloqueada.

3. Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas configurações estejam definidas, os teclados FIDO2 serão automaticamente apresentados nas sessões HDX subsequentes e não exigirão nenhuma ação adicional do usuário final.

### Configurando um mouse 3D usando redirecionamento USB

Atualmente, os drivers do mouse espacial 3dConnexion são suportados apenas em sistemas operacionais de estação de trabalho (Win 10 e Win11). Eles não funcionam em sistemas operacionais de servidor. A seguir estão as etapas para configurar um SpaceMouse Enterprise em um sistema operacional de estação de trabalho (vid=046D, pid=C016).

1. Instale o mais recente driver do Windows no host VDA.
2. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
3. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**.
    a. Defina as informações de **VID** e **PID** para o bloco de assinatura que precisa ser redirecionado e clique em **Salvar**. Por exemplo: **Conectar**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Edite a configuração de política **Regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo junto com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=046D PID=C016 class=03 #Dispositivo de entrada operando em modo de captura
5. Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

7. Edite a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

### Configurando dois ou mais dispositivos usando redirecionamento USB com regras de dispositivo diferentes

Vários dispositivos podem ser redirecionados dentro da sessão HDX com regras de dispositivo diferentes. Um administrador pode querer redirecionar um dispositivo automaticamente, enquanto oferece uma opção ao usuário final para redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Adicione as informações de **VID** e **PID** dos dois dispositivos a serem redirecionados com a regra de dispositivo apropriada na sessão e clique em **Salvar**.
    b. **Permitir**: VID=0911 PID=0c1c #Microfone de fala Phillips.
    c. **Conectar**: VID=06A8 PID=0043 class=03 # Topaz HSB signature pad
3. Edite a configuração da política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração da política **Permitir que dispositivos USB recém-conectados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas configurações estejam definidas, o pad de assinatura Topaz HSB será automaticamente apresentado em sessões HDX subsequentes e não exigirá nenhuma ação adicional do usuário final. O microfone de fala Phillips, por outro lado, exigirá que o usuário final habilite o redirecionamento no Connection Center ou na guia Dispositivos do CDViewer.

## Solução de problemas

As etapas a seguir devem ser seguidas para solucionar problemas relacionados ao redirecionamento USB:

1. Valide se os requisitos do sistema estão sendo atendidos para o redirecionamento USB. Isso inclui as versões corretas do CVAD e CWA, dispositivos suportados e drivers de dispositivo na plataforma do sistema operacional em questão.
2. Certifique-se de que a configuração seja apropriada com base nas versões e plataformas dos componentes em uso em seu ambiente. Consulte a nota em Configuração de Redirecionamento USB Legado para obter detalhes sobre os componentes que exigem configurações de configuração legadas.
3. Valide se o dispositivo está listado em dispositivos que o cliente enumerou.

    a. Barra de ferramentas de Preferências do Workspace: Observe os dispositivos enumerados na guia Dispositivos da barra de ferramentas Preferências do aplicativo Workspace (clique com o botão direito do mouse no **ícone do CWA > Connection Center > Preferências**… Clique na guia **Dispositivos**).

    b. `CtxUsbDiagnostics.exe` (Recomendado): Execute esta ferramenta em uma janela de prompt de comando. A saída fornece informações específicas do dispositivo para uma sessão específica. Ela informará se um dispositivo está sendo redirecionado ou não. Também informará se um conjunto de regras de dispositivo está impedindo o redirecionamento do dispositivo. Consulte Ferramenta de Diagnóstico para obter mais informações.

    c. USBView ou outras ferramentas de terceiros: Execute uma ferramenta de terceiros como o USBView na máquina do endpoint/cliente para garantir que o dispositivo seja detectado no endpoint.

4. Se você vir o dispositivo sendo enumerado:

    a. Se você vir uma regra de Negação na saída da ferramenta CtxUsbDiagnostics para um dispositivo específico, verifique as políticas configuradas no Studio e certifique-se de que as regras estejam definidas corretamente na política da Versão 2. Se a regra de negação não aparecer na política do Studio, verifique a política do lado do cliente e, finalmente, os padrões do lado do cliente nessa ordem para encontrar a regra de negação correspondente.

    b. Se não houver regra de negação na saída do CtxUsbDiagnostics, o CWA permitirá o redirecionamento do dispositivo verificando/clicando no botão apropriado na guia

dispositivos da janela Preferências (Dispositivos > Gerenciar dispositivos). Um dispositivo, uma vez redirecionado, estará disponível na sessão. Isso pode ser verificado consultando o gerenciador de dispositivos/USBView ou aplicativo similar na sessão HDX.

5. Se você não vir o dispositivo sendo apresentado dentro da sessão:

    a. É possível que o driver de dispositivo correto não esteja instalado corretamente no host VDA. Certifique-se de que as versões mais recentes dos drivers de dispositivo estejam instaladas corretamente no host VDA. Alguns drivers de dispositivo não são suportados em máquinas de servidor de terminal, portanto, certifique-se de que não seja esse o caso com o dispositivo que você está tentando redirecionar.

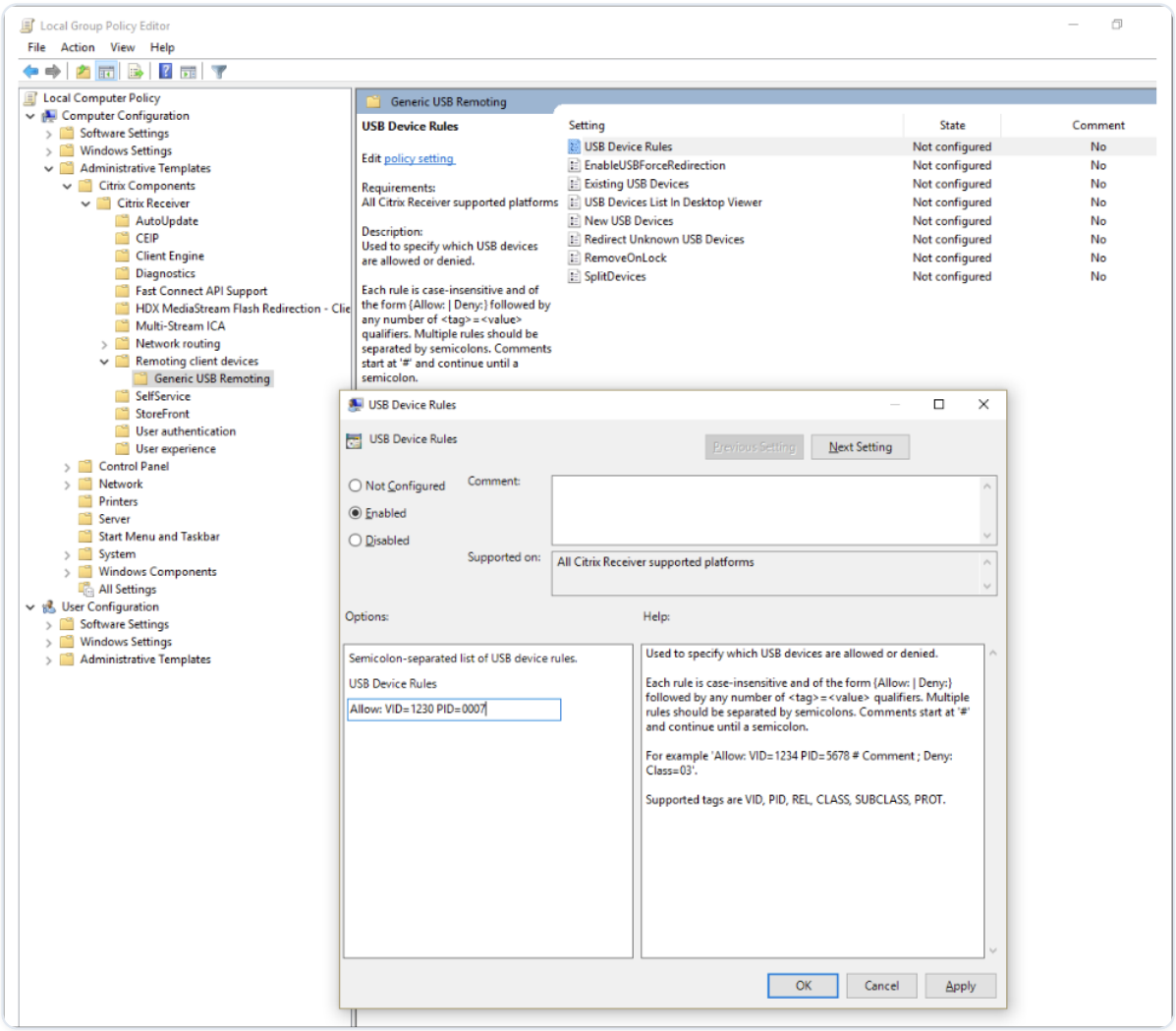
    b. Certifique-se de que o dispositivo não esteja sendo usado no endpoint do cliente. Alguns dispositivos exigem que os drivers sejam instalados também no endpoint do cliente, e isso pode impedi-los de serem redirecionados na sessão.

6. Valide se as regras relacionadas ao USB estão definidas corretamente no endpoint do cliente:

    a. **CWA para Windows**:

        i. Validar se a política de grupo no cliente (adicionar mais detalhes e SS para isso) está configurada apropriadamente e não entra em conflito com as regras definidas no Studio.

        ii. Validar as regras padrão no registro do cliente.




`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA para Linux - Para solucionar problemas do CWA para Linux, consulte a documentação USB para CWA para Linux

c. CWA para Mac - Para solucionar problemas do CWA para Mac, consulte CWA para Mac

**Observação:**

- No TSVDA, os dispositivos de áudio são bloqueados por padrão de usar o redirecionamento USB. A maneira recomendada de usar esses dispositivos é utilizando o VC de Áudio otimizado.
- Às vezes, dispositivos USB compostos podem não ser divididos automaticamente, mesmo que uma regra de redirecionamento de dispositivo correta esteja configurada para dividir o dispositivo. Esse problema ocorre porque o dispositivo está em modo de

baixo consumo de energia. Nessas instâncias, o dispositivo filho que entra no modo de baixo consumo de energia pode não estar presente na lista de dispositivos. Você pode usar as seguintes soluções alternativas para superar esse problema:

  - Desconecte a sessão, insira o dispositivo USB e reconecte-se à sessão.
  - Desconecte o dispositivo USB e conecte-o novamente. Essa ação faz com que o dispositivo saia do modo de baixo consumo de energia.

- Às vezes, as configurações de economia de bateria USB podem estar ativadas para otimizar a vida útil da bateria. Se o endpoint do cliente entrar em suspensão, o dispositivo USB poderá ser desconectado. Nesse cenário, talvez seja necessário desconectar e reconectar o dispositivo para apresentá-lo novamente na sessão.

### Logs de Eventos

Os administradores agora podem monitorar dispositivos não autorizados que os usuários podem tentar redirecionar e podem tomar a ação apropriada. Aqui estão algumas das mensagens de evento que serão registradas no Visualizador de Eventos no host VDA para dispositivos que podem ser redirecionados e para dispositivos que não podem.

| | |
|---|---|
| **Id** | 1000 |
| **Name** | UsbEventAcceptDevice |
| **Severity** | Informational |
| **Facility** | System |
| **Text** | The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted. |
| **Comment** | This message logs the device info of a device redirected in an HDX session |

| | |
|---|---|
| **Id** | 1001 |
| **Name** | UsbEventPolicyRejectsDeviceV1 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule. |
| **Arguments** | |

| | |
|---|---|
| **Id** | 1002 |
| **Name** | UsbEventPolicyRejectsDeviceV2 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt. |
| **Arguments** | |

## Ferramenta de Diagnóstico USB

`CtxUsbDiagnostics.exe` é uma ferramenta de linha de comando no VDA para ajudar os administradores Citrix a diagnosticar e resolver problemas de redirecionamento de dispositivos USB encontrados no cliente de forma acelerada. Esta ferramenta utilitária coleta informações vitais necessárias para triar problemas de configuração associados a dispositivos USB conectados ao cliente que não estão sendo redirecionados dentro de uma sessão HDX.

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to
```

```
ensure the tool has the necessary permissions to perform system-level
operations.
```

## Requisitos

### Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ Versão 2311 ou posterior

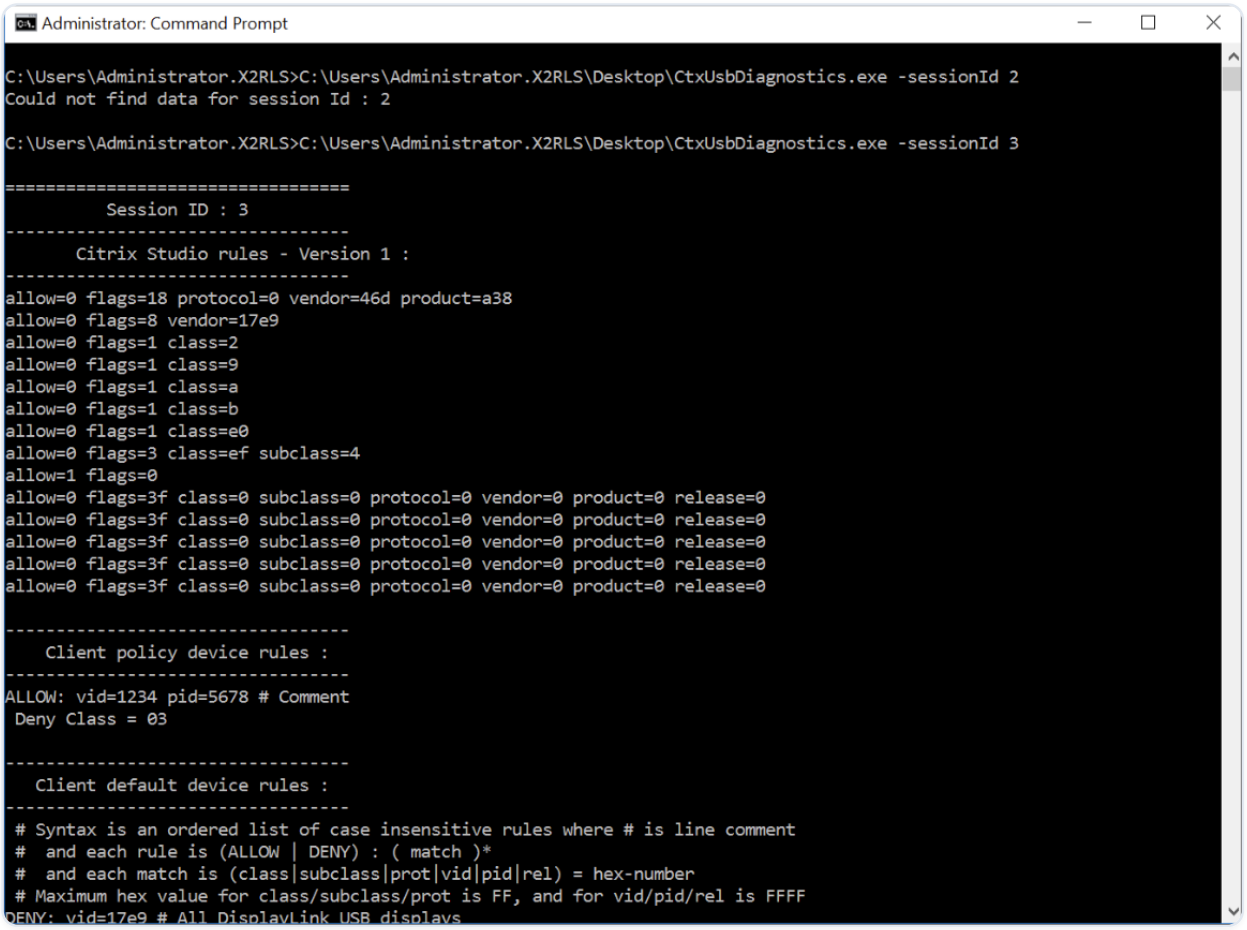
### Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Workspace App
  - Windows: versão 2311 ou posterior

## O que a ferramenta faz?

A ferramenta atualmente fornece:

- SessionID
- Políticas de dispositivo VDA (regras de dispositivo definidas no Studio)
- Dispositivos cliente e políticas de dispositivo cliente (regras de dispositivo)
- Lista de dispositivos, seu estado de redirecionamento e por que foram permitidos ou negados




> **Nota :**
>
> O administrador pode ver informações do dispositivo para todas as sessões ativas.

### Informações Exibidas

- **Regras do Citrix Studio - Versão 1/2**
  - As regras do DDC indicam o uso da política legada “**Regras de redirecionamento de dispositivo USB do cliente**” ou “**Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**” no Studio. As informações listadas nesta seção listam todas as regras configuradas pelo administrador Citrix®.

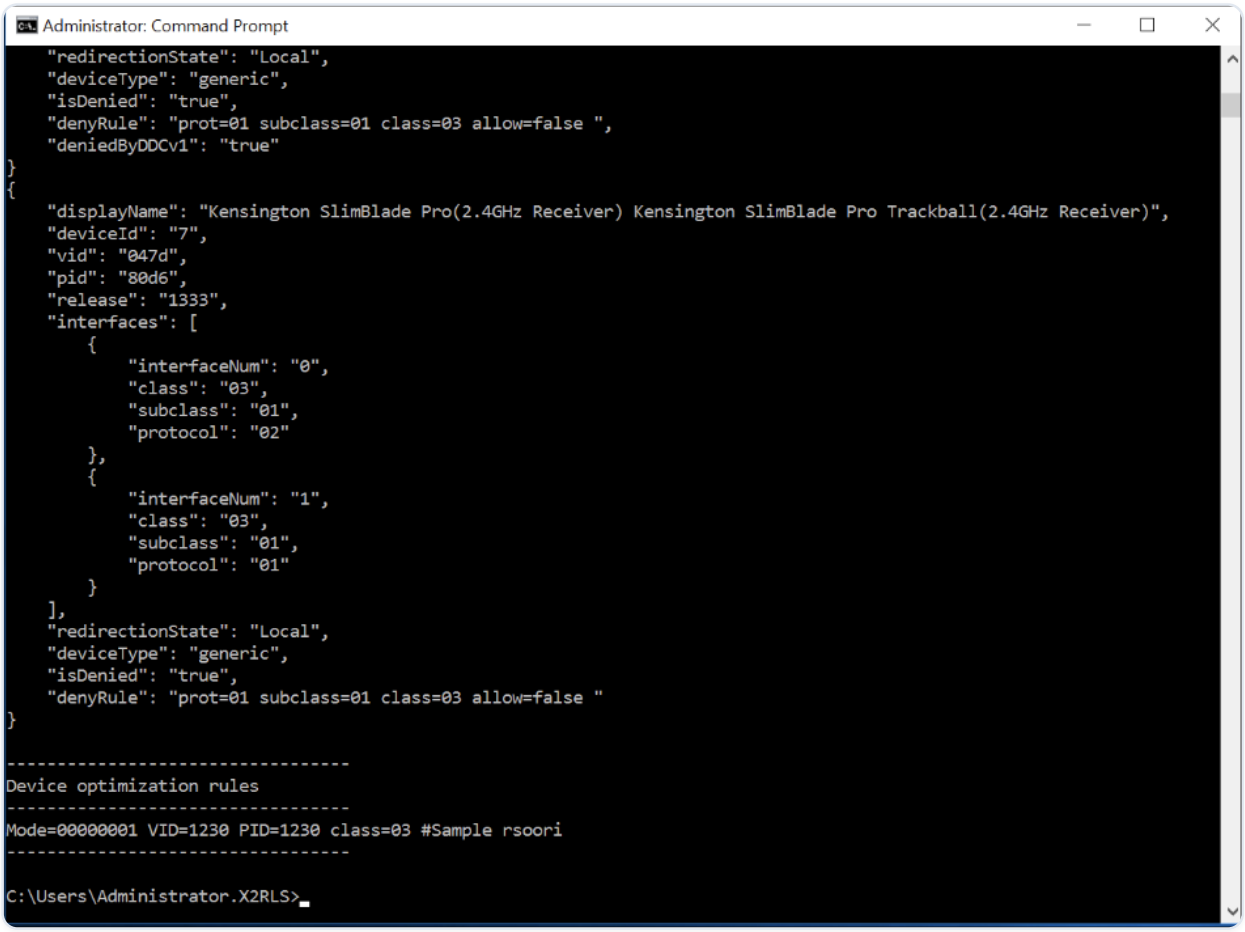
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Regras Padrão de Dispositivo do Cliente**
  - Esta seção lista as regras que são definidas no registro no cliente.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Regras de otimização de dispositivo**
  - A seção lista as regras de otimização de dispositivo conforme definido em "Regras de otimização de dispositivo USB do cliente.




## Lista de Dispositivos

Esta seção lista informações valiosas sobre cada dispositivo conectado ao endpoint do cliente, as informações de hardware, se ele está sendo redirecionado ou não, se a regra de redirecionamento de dispositivo correta está definida ou não, e assim por diante.

| NOME DA TAG | DESCRIÇÃO |
|---|---|
| displayName | Lista o nome comum do dispositivo. |
| ID do fornecedor | ID do Fornecedor |
| ID do produto | ID do Produto |
| Interfaces | Esta subseção lista todas as interfaces caso o dispositivo composto tenha sido dividido em vários dispositivos filhos. |
| InterfaceNum | Indica o índice do descritor da interface |
| classe | Código da Classe |

| NOME DA TAG | DESCRIÇÃO |
|---|---|
| subclasse | Código da Subclasse |
| protocolo | Protocolo |
| redirectionState | **Local** indica que o dispositivo não é redirecionado na sessão ICA®. **ThisSession** indica que o dispositivo é redirecionado na sessão ICA. **OtherSession** indica que o dispositivo é redirecionado em outra sessão ICA. |
| optiEnabled | **true** indica que o dispositivo está otimizado. **false** indica que o dispositivo não está otimizado e a transferência de dados ocorre através do canal virtual USB. |
| deviceType | **generic** indica que o dispositivo não possui um canal virtual otimizado e o tráfego está fluindo através do canal virtual USB. **optimized** implica que a transferência de dados associada ao dispositivo está ocorrendo através de um canal virtual dedicado. |
| isDenied | **true** indica que o dispositivo não é redirecionado devido a uma regra de política definida pelo administrador. `false` indica que o dispositivo é redirecionado devido à política aplicada. |
| denyRule | Este campo é útil se **isDenied** estiver definido como `true`. Ele informa ao administrador o conjunto de regras específico na política que está impedindo o redirecionamento do dispositivo. |

## Configuração de Redirecionamento USB Legado

Se você estiver usando componentes anteriores à versão 2212 ou se estiver usando o CWA para Linux, siga este guia para configurar o redirecionamento USB em seu ambiente.

### Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.
3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

### Criando Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em relação a cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de Permissão, o dispositivo correspondente terá permissão para ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

**Configurando a política no DDC:**

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente**.
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar. Por exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Mass Storage

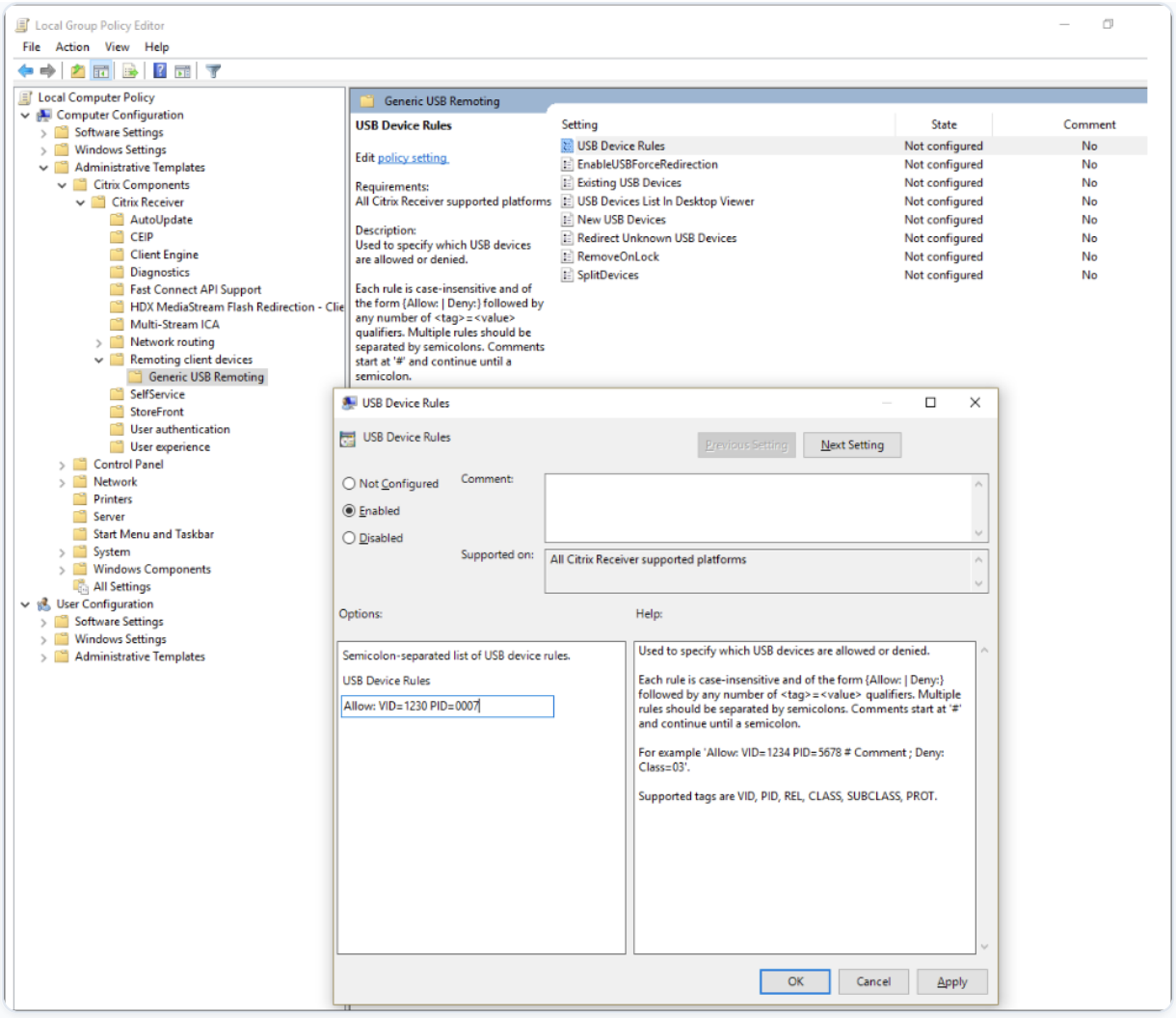
> **Nota:**
>
> Se um administrador Citrix® marcar Usar valor padrão e clicar em Salvar, as regras padrão poderão ser encontradas no seguinte registro no VDA.
>
> **Cuidado!:**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

**Usando GPOs no cliente:**

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
2. Abra a **configuração de Regras de Dispositivo USB** e ative a configuração. Adicione a regra de Dispositivo USB como neste exemplo, A regra Permitir: VID=1230 PID=0007 permite o dispositivo com ID de Fornecedor 1230 e ID de Produto 0007.

**Nota:**

Use a regra Permitir: VID=xxxx PID=xxxx quando um dispositivo específico deve estar no topo da lista de regras de dispositivo.




**Nota:**

> Uma ferramenta como USBView ou até mesmo a barra de ferramentas de Conexão pode ser usada para determinar os detalhes do dispositivo, como VID e PID (inclua SS aqui).

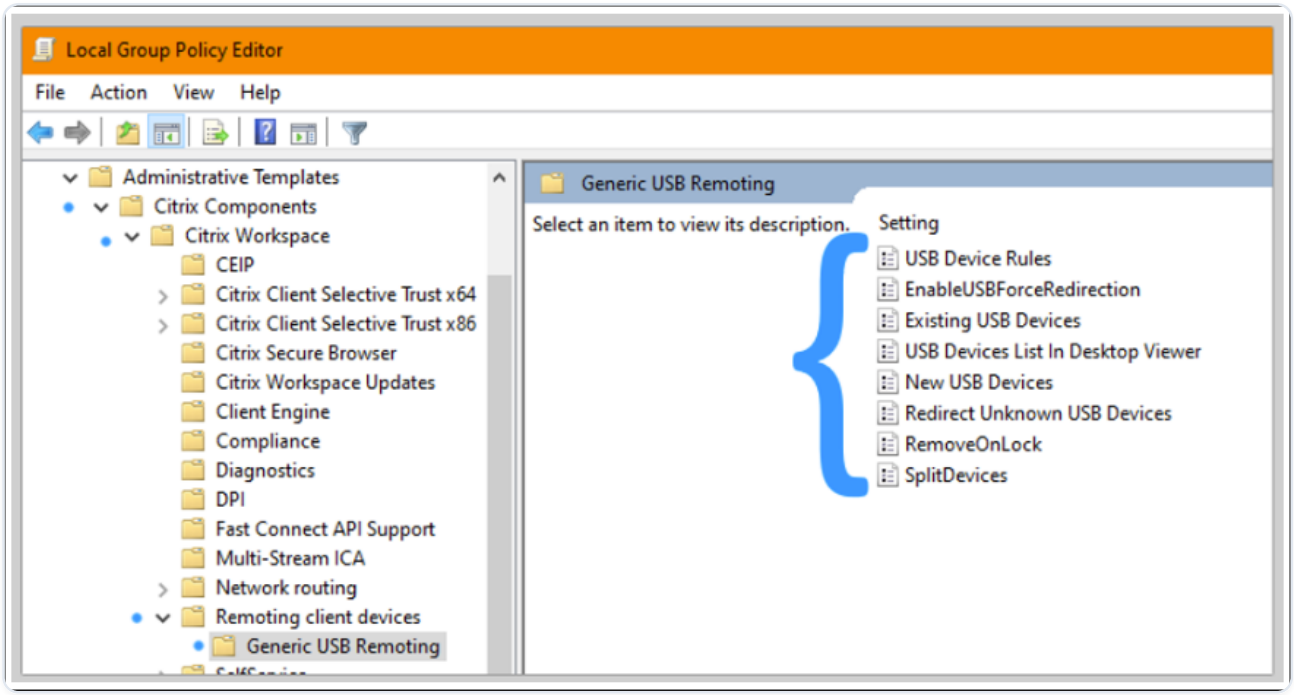
### Configurar o redirecionamento automático de dispositivos USB

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use a configuração de política DeviceRules no endpoint do cliente.

Esta política pode ser definida no cliente usando um GPO, registro do lado do cliente, usando as Preferências do Citrix Workspace™ ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

**Usando GPOs no cliente:**

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
2. Abra **Novos Dispositivos USB**, selecione **Ativado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Ativado** e clique em **OK**.

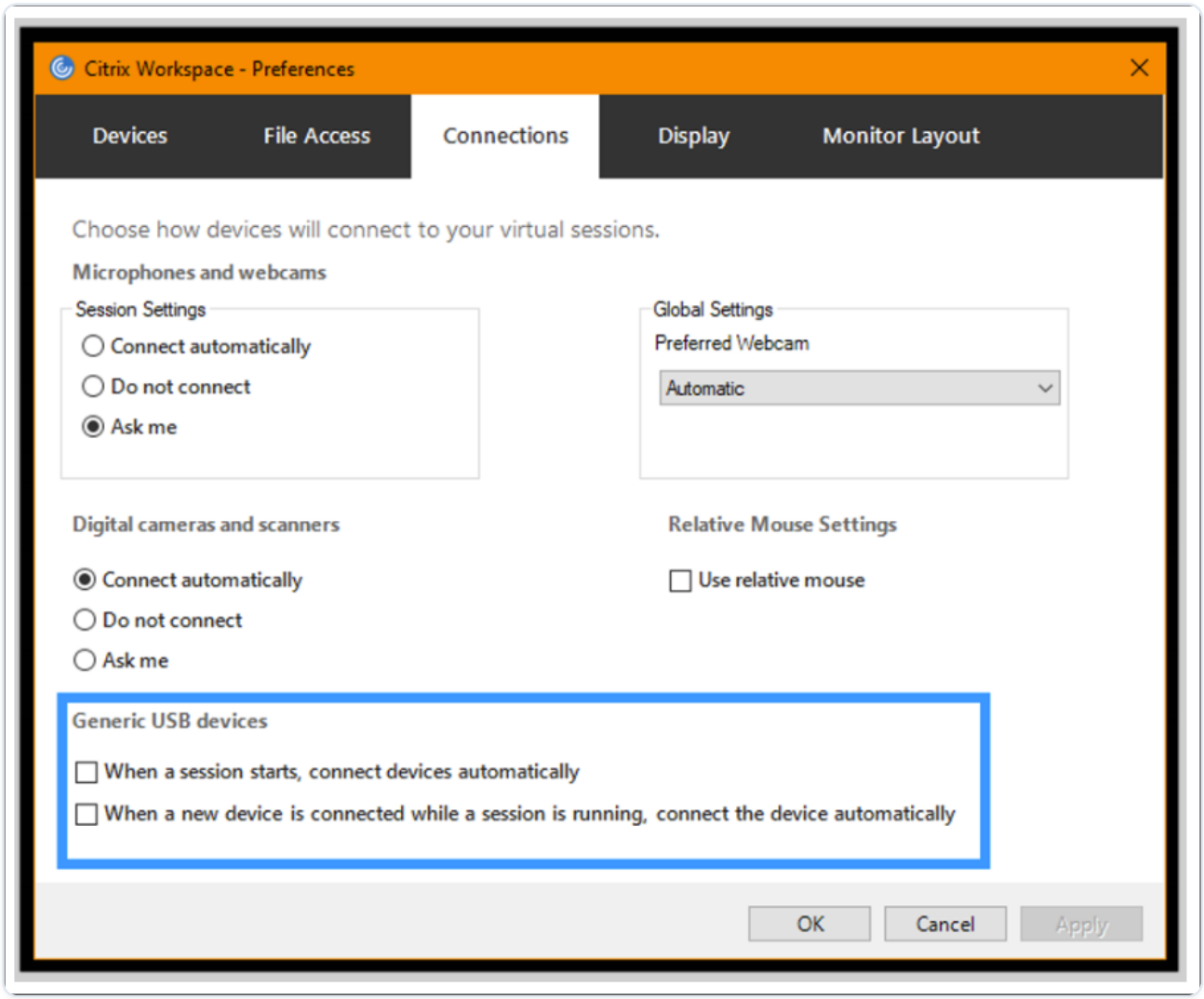



**Usando o Citrix Connection Center:**

1. Vá para **Citrix Workspace Preferences > Connections**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão iniciar, conectar dispositivos automaticamente
    b. Quando um novo dispositivo for conectado enquanto uma sessão estiver em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

**Usando a barra de ferramentas de conexão do CDViewer:**

1. Após o início de uma sessão, clique no menu suspenso **CDViewer** e selecione a guia **Citrix Workspace Preferences > Connections**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão iniciar, conectar dispositivos automaticamente
    b. Quando um novo dispositivo for conectado enquanto uma sessão estiver em execução, conectar o dispositivo automaticamente.
3. Clique em **Apply** e **OK** para salvar a política.




Para as configurações baseadas no cliente, as chaves de registro são definidas no dispositivo cliente no seguinte local:

> **Cuidado!:**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

### Configurando dois ou mais dispositivos usando o redirecionamento USB com regras de dispositivo diferentes

Vários dispositivos podem ser redirecionados dentro da sessão HDX™ com regras de dispositivo diferentes. Um administrador pode querer redirecionar um dispositivo automaticamente, enquanto oferece uma opção ao usuário final para redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a configuração **Regras de dispositivo USB** no GPO do lado do cliente.
    a. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
    b. Abra a **configuração Regras de Dispositivo USB** e habilite a configuração. Adicione a regra de Dispositivo USB como neste exemplo: A regra **Allow: 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 de Fornecedor 06A8** e **ID de Produto 0043**, desde que as políticas de redirecionamento automático mencionadas na etapa 3 estejam definidas.
    c. **Permitir**: VID=0911 PID=0c1c #Microfone de fala Phillips.
    d. **Conectar**: VID=06A8 PID=0043 class=03 # Mesa digitalizadora Topaz HSB
3. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
4. Abra **Novos Dispositivos USB**, selecione **Habilitado** e clique em **OK**.
5. Abra **Dispositivos USB Existentes**, selecione **Habilitado** e clique em **OK**.

Uma vez que essas configurações estejam configuradas, a mesa digitalizadora Topaz será redirecionada automaticamente dentro da sessão HDX e será necessária uma ação adicional do usuário final (selecionar a opção Redirecionar no centro de Conexão ou na guia Dispositivos do CD Viewer) para redirecionar o microfone de fala Phillips na sessão.

> **Nota:**

> As configurações acima nas etapas 2 e 3 poderiam 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 maneira recomendada.

# Mapeamento de Unidade Cliente (CDM)

O Mapeamento de Unidade Cliente (CDM) disponibiliza unidades de armazenamento no endpoint do cliente dentro de uma sessão Citrix HDX™ para permitir que arquivos e pastas sejam transferidos do cliente para o host da sessão e vice-versa. Esse recurso é habilitado por padrão com privilégios de leitura e gravação. Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, habilite a configuração de política **Acesso somente leitura à unidade cliente**. Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja definida como **Permitido** e também seja adicionada à política.

Como precaução de segurança, as unidades de endpoint são mapeadas sem a permissão de execução por padrão. Para permitir que os usuários executem executáveis diretamente das unidades cliente mapeadas, edite o valor de registro **ExecuteFromMappedDrive** no host da sessão. Para obter detalhes, consulte Unidades cliente mapeadas na seção **Recursos HDX gerenciados por meio do registro**.

## Requisitos

A seguir estão os requisitos para usar o CDM:

### Plano de controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

### Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2016 ou posterior
  - Linux: Consulte os requisitos de sistema do VDA Linux
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 ou posterior
  - Linux: Consulte a documentação do VDA Linux

### Dispositivo cliente

- Sistema operacional

- Windows 10 1809 ou posterior
- Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux

### Políticas relacionadas

Consulte a seção Referência de configurações de política para as configurações de CDM.

### Cenários de salto duplo

O CDM é compatível em cenários de salto duplo. Por padrão, a unidade do endpoint do cliente é mapeada para a sessão do segundo salto e as unidades do primeiro salto não estão disponíveis. No entanto, isso pode ser configurado para que as unidades do primeiro salto sejam mapeadas na sessão do segundo salto em vez das unidades do endpoint do cliente.

Para configurar essa funcionalidade, edite o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- Nome do valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Dados do valor:
  - True - Mapeia as unidades da sessão do primeiro salto na sessão do segundo salto
  - False - Mapeia as unidades do endpoint do cliente na sessão do segundo salto

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

## Suporte para dispositivos cliente móveis e com tela sensível ao toque

O Citrix Virtual Apps and Desktops™ permite que os usuários acessem seus aplicativos e desktops publicados a partir de dispositivos cliente móveis e com tela sensível ao toque.

# Requisitos

### Plano de controle Citrix®

- Citrix Virtual Apps and Desktops 1912 ou posterior
- Citrix DaaS™

### Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows 11 21H2 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops versão 7.15 ou posterior

### Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
- Aplicativo Citrix Workspace™ para Windows versão 1808 ou posterior

## Modo tablet para dispositivos com tela sensível ao toque usando o Windows Continuum

Continuum é um recurso do Windows 10 que se adapta à forma como o dispositivo cliente é usado. Quando o VDA detecta a presença de um teclado ou mouse em um cliente habilitado para toque, ele coloca o cliente no modo desktop. Se um teclado ou mouse não estiver presente, o VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão da sessão e também durante a sessão quando o teclado ou mouse é conectado ou desconectado.

O recurso é habilitado por padrão. Para desabilitar este recurso, configure as configurações de política Configurações de política de alternância do modo tablet.

Além dos requisitos para dispositivos com tela sensível ao toque mencionados acima, os seguintes são necessários para o Windows Continuum:

### XenServer (anteriormente Citrix Hypervisor™)

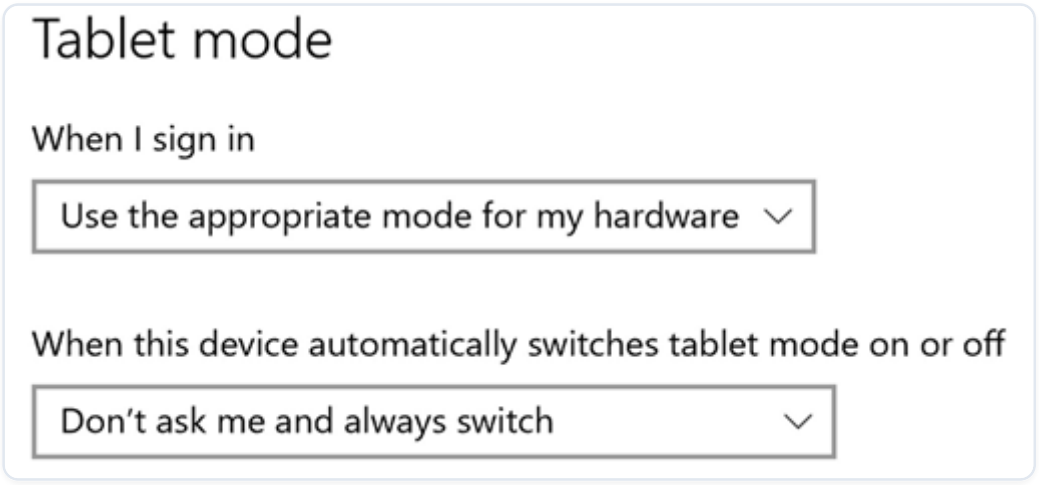
- Citrix Hypervisor 8.2 ou superior
- Execute o comando CLI do XenServer para permitir a alternância entre laptop/tablet: **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **Importante:**

> A atualização da imagem base para um catálogo de máquinas existente após a alteração da configuração de metadados não afeta nenhuma VM provisionada anteriormente. Após alterar a imagem base da VM do XenServer, crie um catálogo, escolha a imagem base e provisione uma nova máquina do Machine Creation Services™ (MCS).

### Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows 11 21H2 ou posterior
- VDA
  - Windows: versão 7.16 ou posterior
  - **Devido às limitações atuais nas configurações do sistema operacional, o usuário terá que definir as seguintes opções nos menus suspensos depois de iniciar a primeira sessão ICA® e reiniciar o VDA:**
    - **Configurações > Sistema > Modo Tablet**
      - Usar o modo apropriado para meu hardware
      - Não me perguntar e sempre alternar




O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores.
- A tela Iniciar e todos os aplicativos que você inicia abrem em tela cheia.
- A barra de tarefas contém um botão Voltar.
- Ícones excluídos da barra de tarefas.

Você tem acesso ao Explorador de Arquivos.



O Windows 10 carrega o driver GPIO na máquina virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro da máquina virtual.

O aplicativo Citrix Workspace para HTML5 não oferece suporte aos recursos do Windows Continuum.

O **modo desktop** oferece a interface de usuário tradicional onde você interage da mesma forma que usando um PC, teclado e mouse.

# Canetas Microsoft Surface Pro e Surface Book

Oferecemos suporte à funcionalidade padrão da caneta com aplicativos baseados em Windows Ink. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e do modelo da caneta. Por exemplo, a pressão da caneta pode ter até 4096 níveis. Este recurso é ativado por padrão.

A seguir estão os requisitos para o suporte à funcionalidade da caneta:

### Plano de controle Citrix

- Citrix Virtual Apps and Desktops 1903 ou posterior
- Citrix DaaS

### Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1903 ou posterior

### Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
- Citrix Workspace app para Windows versão 1902 ou posterior

Para uma demonstração do Windows Ink e da funcionalidade da caneta, clique neste gráfico:



Para desabilitar ou habilitar esse recurso, consulte Canetas Microsoft Surface Pro e Surface Book na lista de recursos gerenciados pelo registro.

### Problemas conhecidos

A seguir estão os problemas conhecidos com o suporte à caneta:

- Devido a limitações do SO no Windows Server 2k22, os usuários não conseguirão definir atalhos de caneta ou fazer ajustes nas configurações de caneta/tinta no Painel de Controle ao se conectar a aplicativos ou desktops do servidor 2k22.
- Os atalhos de caneta não estão sendo respeitados de um cliente Windows 11 habilitado para caneta devido a uma limitação do sistema operacional.

## Portas seriais

A maioria dos PCs novos não possui portas seriais (COM) integradas. As portas são fáceis de adicionar usando conversores USB. Aplicativos adequados para portas seriais geralmente envolvem sensores, controladores, leitores de cheque antigos, pads e assim por diante. Alguns dispositivos USB de porta COM virtual usam drivers específicos do fornecedor em vez dos drivers fornecidos pelo Windows (usbser.sys). Esses drivers permitem que você force a porta COM virtual do dispositivo USB para que ela não mude mesmo se conectada a diferentes soquetes USB. Isso pode ser feito em **Gerenciador de Dispositivos > Portas (COM e LPT) > Propriedades** ou no aplicativo que controla o dispositivo.

O mapeamento de porta COM do cliente permite que dispositivos conectados às portas COM no endpoint do usuário sejam usados durante sessões virtuais. Você pode usar esses mapeamentos como qualquer outro mapeamento de rede.

Para cada porta COM, um driver no sistema operacional atribui um nome de link simbólico, como COM1 e COM2. Os aplicativos então usam o link para acessar a porta.

> **Importante:**

> O fato de um dispositivo poder ser conectado ao endpoint usando USB diretamente não significa que ele possa ser redirecionado usando o redirecionamento USB genérico. Alguns dispositivos USB funcionam como portas COM virtuais, que os aplicativos podem acessar da mesma forma que uma porta serial física. O sistema operacional pode abstrair portas COM e tratá-las como compartilhamentos de arquivos. Dois protocolos comuns para COM virtual são CDC ACM ou MCT. Quando conectados por meio de uma porta RS-485, os aplicativos podem não funcionar. Obtenha um conversor RS-485 para RS232 para usar RS-485 como uma porta COM. **Importante:**

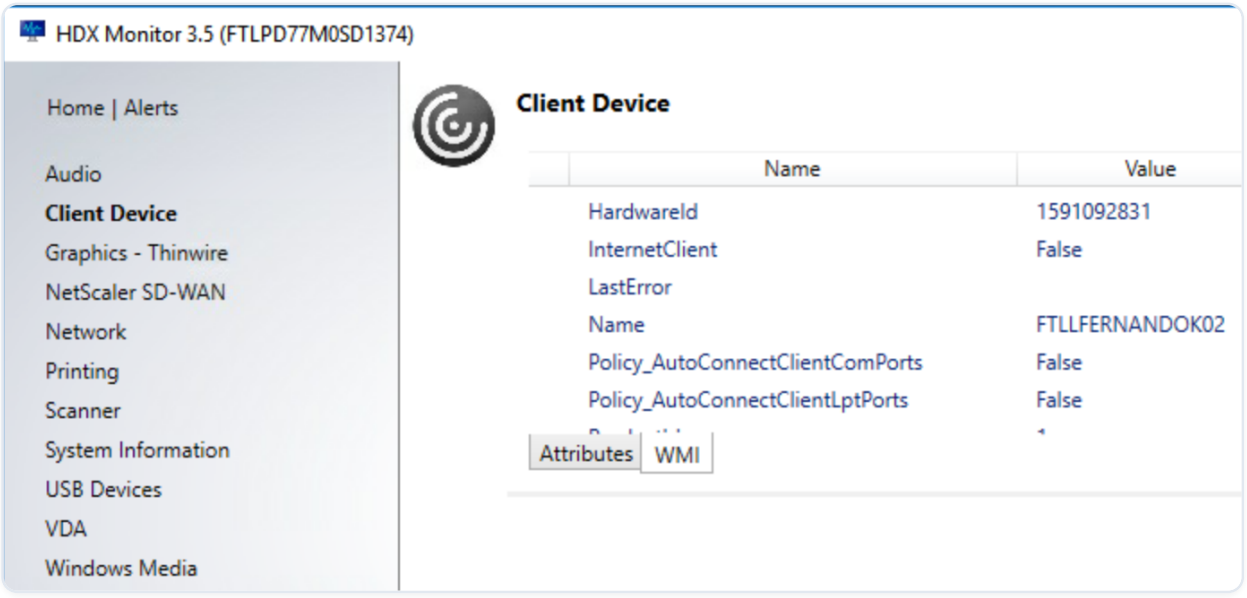
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um pad de assinatura) de forma consistente apenas se ele estiver conectado a COM1 ou COM2 na estação de trabalho cliente.

## Mapear uma porta COM do cliente para uma porta COM do servidor

Você pode mapear portas COM do cliente para uma sessão Citrix® de três maneiras:

- Políticas do Studio. Para obter mais informações sobre políticas, consulte Configurações de política de redirecionamento de porta.
- Prompt de comando do VDA.
- Ferramenta de configuração da Área de Trabalho Remota (Serviços de Terminal).

1. Habilite as políticas **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente do Studio**. Após aplicadas, algumas informações estarão disponíveis no HDX™ Monitor.




2. Se a **Conexão automática de portas COM do cliente** falhou ao mapear a porta, você pode mapear a porta manualmente ou usar scripts de logon. Faça logon no VDA e, em uma janela de prompt de comando, digite:

   NET USE COMX: `\\CLIENT\COMZ`:

   Ou

   NET USE COMX: `\\CLIENT\CLIENTPORT:COMZ`:

**X** é o número da porta COM no VDA (as portas de 1 a 9 estão disponíveis para mapeamento). **Z** é o número da porta COM do cliente que você deseja mapear.

Para confirmar que a operação foi bem-sucedida, digite **NET USE** em um prompt de comando do VDA. A lista que aparece contém unidades mapeadas, portas LPT e portas COM mapeadas.




3. Para usar esta porta COM em um desktop ou aplicativo virtual, instale o aplicativo do seu dispositivo de usuário e aponte-o para o nome da porta COM mapeada. Por exemplo, se você mapear COM1 no cliente para COM3 no servidor, instale o aplicativo do seu dispositivo de porta COM no VDA e aponte-o para COM3 durante a sessão. Use esta porta COM mapeada como usaria uma porta COM no dispositivo do usuário.

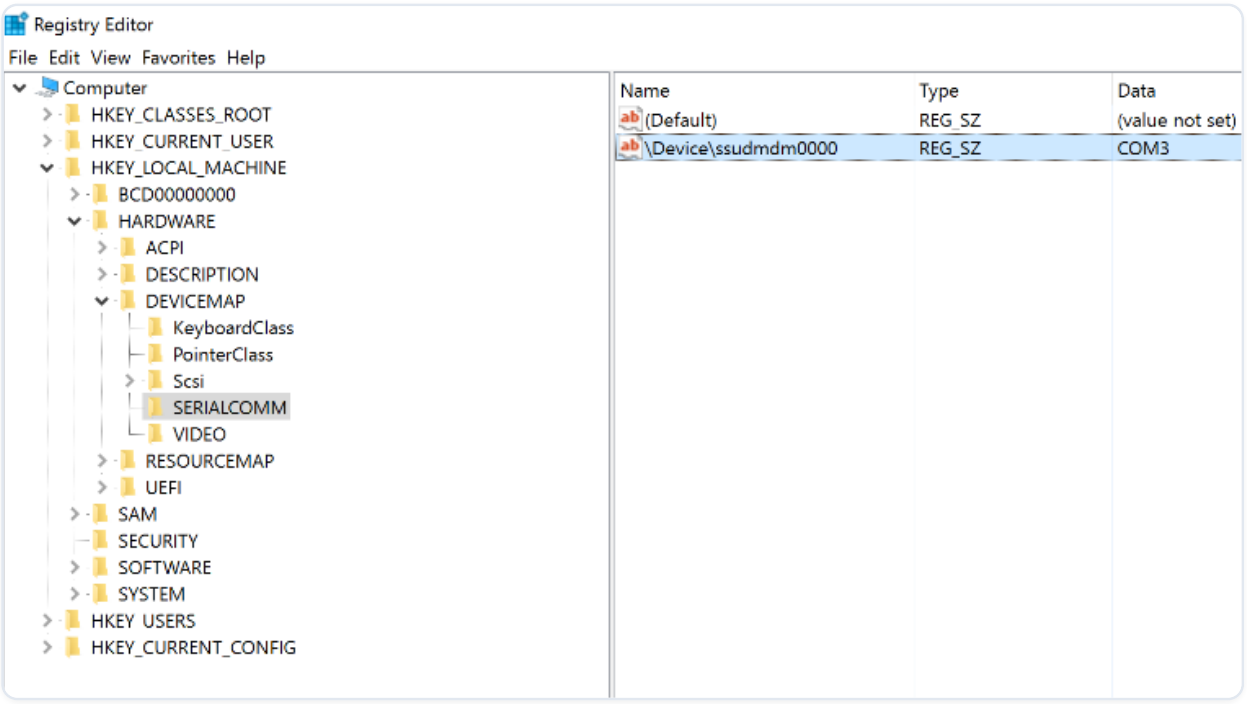
**Importante:**

O mapeamento de porta COM não é compatível com TAPI. Você não pode mapear dispositivos da Interface de Programação de Aplicativos de Telefonia do Windows (TAPI) para portas COM do cliente. TAPI define uma maneira padrão para os aplicativos controlarem as funções de telefone para chamadas de dados, fax e voz. TAPI gerencia a sinalização, incluindo discagem, atendimento e encerramento de chamadas. Além disso, serviços suplementares como retenção, transferência e chamadas em conferência.

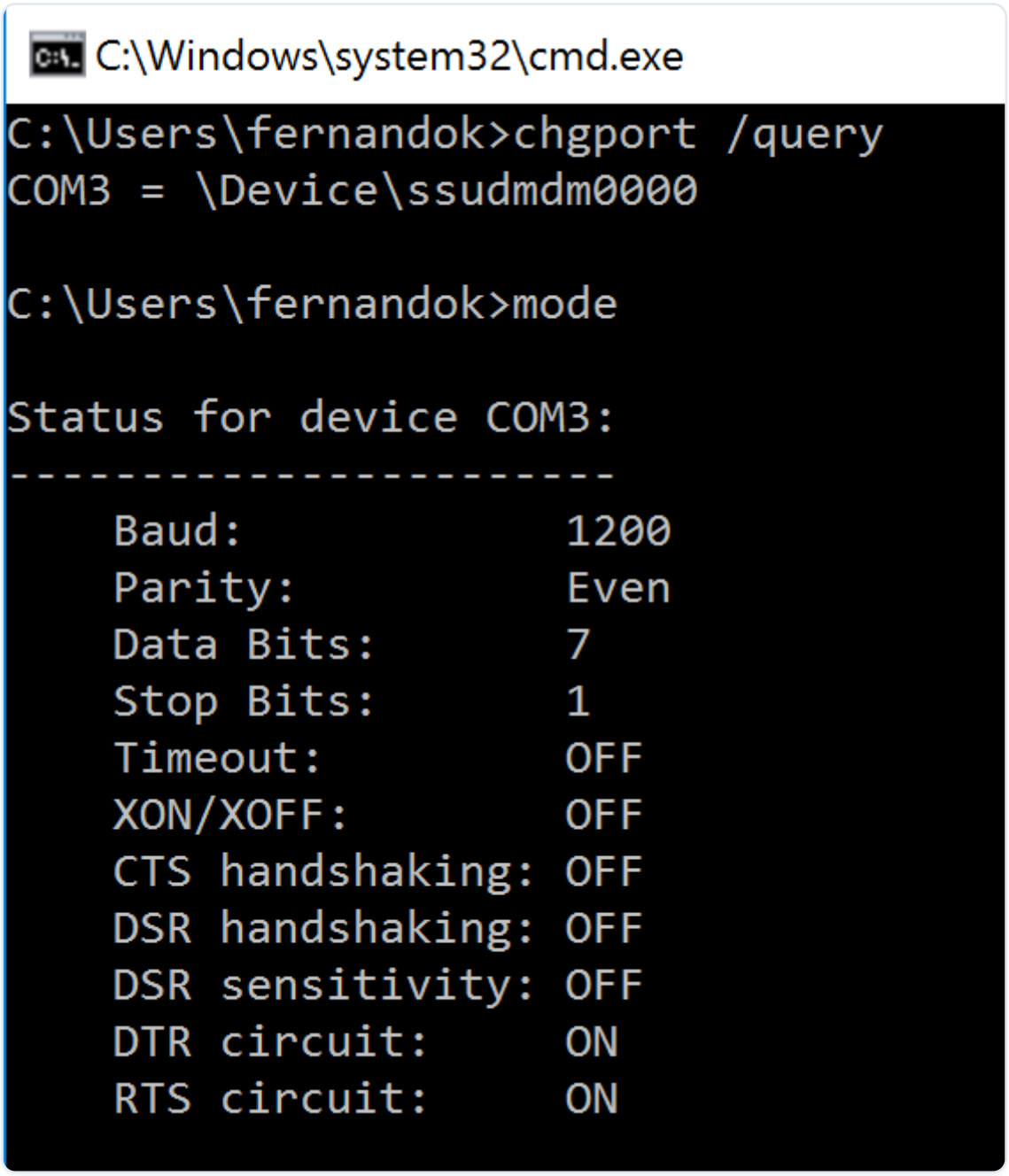
## Solução de problemas

1. Certifique-se de que você pode acessar o dispositivo diretamente do endpoint, ignorando o Citrix. Enquanto a porta não estiver mapeada para o VDA, você não estará conectado a uma sessão Citrix. Siga todas as instruções de solução de problemas que vieram com o dispositivo e verifique se ele funciona localmente primeiro. Quando um dispositivo é conectado a uma

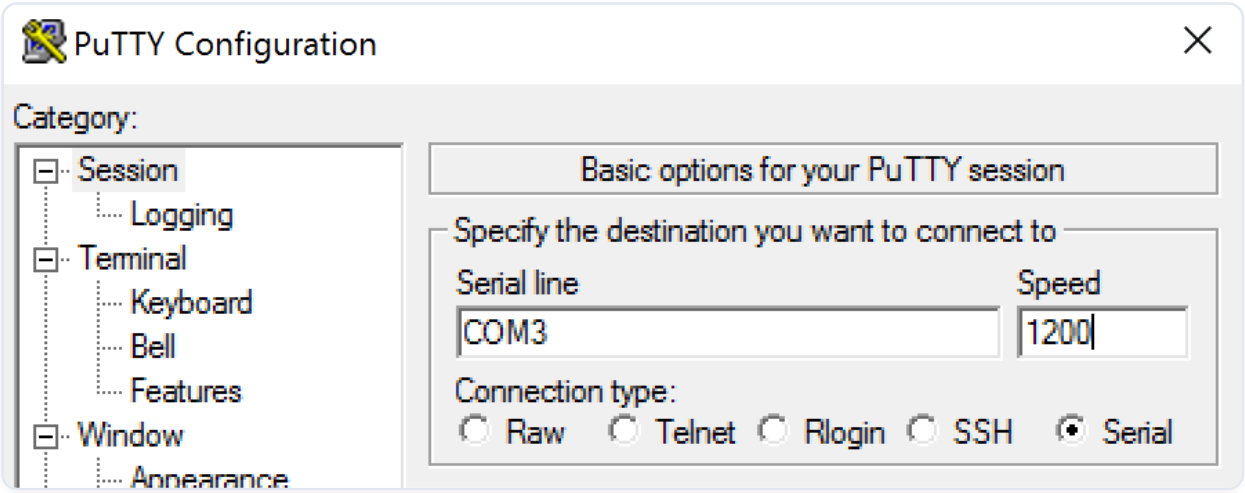
porta COM serial, uma chave de registro é criada no hive mostrado aqui:




Você também pode encontrar essas informações no prompt de comando executando **chgport /query**.




Se as instruções de solução de problemas para o dispositivo não estiverem disponíveis, tente abrir uma sessão PuTTY. Escolha **Session** e em **Serial line** especifique sua porta COM.



Você pode executar **MODE** em uma janela de comando local. A saída pode exibir a porta COM em uso e os valores de Baud/Paridade/Bits de Dados/Bits de Parada, que você precisa em sua sessão PuTTY. Se a conexão PuTTY for bem-sucedida, pressione **Enter** para ver o feedback do dispositivo. Quaisquer caracteres que você digitar podem ser repetidos na tela ou respondidos. Se esta etapa não for bem-sucedida, você não poderá acessar o dispositivo a partir de uma sessão virtual.

2. Mapeie a porta COM local para o VDA (usando políticas ou **NET USE COMX: `\\CLIENT\COMZ`:**) e repita os mesmos procedimentos do PuTTY da etapa anterior, mas desta vez a partir do PuTTY do VDA. Se o PuTTY não conseguir exibir o erro **Unable to open connection to COM1. Unable to open serial port**, outro dispositivo pode estar usando a COM1.
3. Execute **chgport /query**. Se o driver serial integrado do Windows no VDA estiver atribuindo automaticamente \Device\Serial0 a uma porta COM1 do seu VDA, faça o seguinte: A. Abra o CMD no VDA e digite **NET USE.**

   B. Exclua qualquer mapeamento existente (por exemplo, COM1) no VDA.

   **NET USE COM1 /DELETE**

   C. Mapeie o dispositivo para o VDA.

   **NET USE COM1: `\\CLIENT\COM3`:**

   D. Aponte seu aplicativo no VDA para COM3.

   Por fim, tente mapear sua porta COM local (por exemplo, COM3) para uma porta COM diferente no VDA (que não seja a COM1, por exemplo, COM3). Certifique-se de que seu aplicativo esteja apontando para ela: **NET USE COM3: `\\CLIENT\COM3`**
4. Se agora você vir a porta mapeada, o PuTTY estiver funcionando, mas nenhum dado estiver passando, pode ser uma condição de corrida. O aplicativo pode se conectar e abrir a porta antes que ela seja mapeada, impedindo que seja mapeada. Tente uma das seguintes opções:

   - Abra um segundo aplicativo publicado no mesmo servidor. Aguarde alguns segundos para que a porta seja mapeada e, em seguida, abra o aplicativo real que tenta usar a porta.
   - Habilite as políticas de redirecionamento de porta COM no Editor de Política de Grupo no Active Directory em vez do Studio. Essas políticas são **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente**. As políticas aplicadas dessa forma podem ser processadas antes das políticas do Studio, garantindo que a porta

COM seja mapeada. As políticas Citrix são enviadas para o VDA e armazenadas em: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- Use este script de logon para o usuário ou, em vez de publicar o aplicativo, publique um script .bat que primeiro exclui qualquer mapeamento no VDA, mapeia novamente a porta COM virtual e, em seguida, inicia o aplicativo:

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\ \CLIENT\COM1`: NET USE COM2: `\\CLIENT\COM2`: MODE COM1: BAUD=1200 (ou qualquer valor necessário) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (ou qualquer valor necessário) START C:\Program Files\\\<Your Software Path>\\ \<your_software.exe>

5. O Process Monitor da Sysinternals é a ferramenta de último recurso. Ao executar a ferramenta no VDA, localize e filtre objetos como COM3, picaser.sys, CdmRedirector, mas especialmente \<your_app\>.exe. Quaisquer erros podem aparecer como Acesso Negado ou similar.

# Teclados especializados

## Teclados Bloomberg

**Aviso:**

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

O Citrix Virtual Apps and Desktops™ oferece suporte ao teclado Bloomberg modelo 5, modelo 4 Starboard (e ao modelo 3 anterior). Este teclado permite que clientes do setor financeiro usem os recursos especiais do teclado para acessar dados do mercado financeiro e realizar negociações rapidamente.

**Importante:**

> Recomendamos que você use o teclado Bloomberg com apenas uma sessão. Não recomendamos o uso do teclado com várias sessões simultâneas (um cliente para várias sessões).

> O teclado Bloomberg é um dispositivo composto USB que compreende vários dispositivos USB em um único invólucro físico:

- Teclado.
- Leitor de impressão digital.
- Dispositivo de áudio com teclas para aumentar e diminuir o volume e silenciar o alto-falante e o microfone. Este dispositivo inclui alto-falante integrado, microfone e conector para microfone e fone de ouvido.
- Hub USB para conectar todos esses dispositivos ao sistema.

**Requisitos:**

- A sessão à qual o aplicativo Citrix Workspace™ para Windows está se conectando deve oferecer suporte a dispositivos USB.
- Mínimo de Citrix Workspace app 2207 para Linux para oferecer suporte ao teclado Bloomberg modelo 5.
- Mínimo de Citrix Workspace app 2109 para Windows para oferecer suporte ao teclado Bloomberg modelo 5.
- Mínimo de Citrix Workspace app 1808 para Windows ou Citrix Receiver para Windows 4.8 para oferecer suporte aos teclados Bloomberg modelos 3 e 4.
- Mínimo de Citrix Workspace app 1808 para Windows ou Citrix Receiver para Windows 4.12 para usar o modo KVM (dois cabos USB, um roteado através do KVM) para o Modelo 4.

Para obter informações sobre como configurar teclados Bloomberg no aplicativo Citrix Workspace para Windows, consulte Configurando teclados Bloomberg.

Para habilitar o suporte ao teclado Bloomberg, consulte Teclados Bloomberg na lista de recursos gerenciados através do registro.

**Verificar suporte:**

Para determinar se o suporte ao teclado Bloomberg está habilitado no Citrix Workspace app, verifique se o Desktop Viewer relata corretamente os dispositivos do teclado Bloomberg.

Cenário de desktop:

Abra o Desktop Viewer. Se o suporte ao teclado Bloomberg estiver habilitado, o Desktop Viewer mostrará três dispositivos sob o ícone USB:

Para teclado Bloomberg 5:

- Módulo Biométrico Bloomberg LP Bloomberg
- Teclado Bloomberg LP (Dispositivo composto com duas interfaces)
- Áudio do Teclado Bloomberg LP (Dispositivo composto com três interfaces)

Para teclados Bloomberg 3 e 4:

- Scanner de Impressão Digital Bloomberg
- Recursos do Teclado Bloomberg
- Teclado Bloomberg LP 2013

Cenário apenas de aplicativo Seamless:

Abra o menu **Connection Center** a partir do ícone da área de notificação do aplicativo Citrix Workspace. Se o suporte ao teclado Bloomberg estiver habilitado, os três dispositivos aparecerão no menu **Devices**.

A marca de seleção ao lado de cada um desses dispositivos indica que eles são redirecionados para a sessão.

# Webcams

## Streaming de webcam de alta definição

Webcams podem ser usadas por aplicativos de videoconferência executados dentro da sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo de videoconferência. Quando a webcam e o aplicativo suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos resoluções de webcam de até 1920x1080.

Este recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para obter uma lista de plataformas do aplicativo Citrix Workspace que suportam o redirecionamento de webcam HDX, consulte Matriz de recursos do aplicativo Citrix Workspace.

Para obter mais informações sobre streaming de webcam de alta definição, consulte videoconferência HDX e compactação de vídeo de webcam.

Você pode usar uma chave de registro para desabilitar e habilitar o recurso e, em seguida, configurar uma resolução específica. Para obter informações, consulte Streaming de webcam de alta definição e Resolução de webcam de alta definição na lista de recursos gerenciados por meio do registro.

# Gráficos

Os gráficos Citrix HDX incluem um extenso conjunto de tecnologias de aceleração e codificação gráfica que otimizam a entrega de aplicativos gráficos ricos do Citrix Virtual Apps and Desktops. As tecnologias gráficas proporcionam a mesma experiência de usar um desktop físico ao trabalhar remotamente com aplicativos virtuais que são intensivos em gráficos.

Você pode usar software ou hardware para renderização gráfica. A renderização por software requer uma biblioteca de terceiros chamada rasterizador de software. Por exemplo, o Windows inclui o rasterizador WARP para gráficos baseados em DirectX. Às vezes, você pode querer usar um renderizador de software alternativo. A renderização por hardware (aceleração de hardware) requer um processador gráfico (GPU).

O HDX™ Graphics oferece uma configuração de codificação padrão otimizada para os casos de uso mais comuns. Usando as políticas da Citrix, os administradores de TI também podem configurar várias configurações relacionadas a gráficos para atender a diferentes requisitos e proporcionar a experiência de usuário desejada.

### Thinwire

Thinwire é a tecnologia de acesso remoto de exibição padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de acesso remoto de exibição permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição. Os gráficos são gerados como resultado da entrada do usuário, por exemplo, toques de tecla ou ações do mouse.

### HDX 3D Pro

Os recursos do HDX 3D Pro no Citrix Virtual Apps and Desktops permitem que você entregue desktops e aplicativos que têm o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta aceleração de GPU apenas para DirectX.

### Aceleração de GPU para SO de sessão única do Windows

Ao usar o HDX 3D Pro, você pode entregar aplicativos graficamente intensivos como parte de desktops ou aplicativos hospedados em máquinas de SO de sessão única. O HDX 3D Pro suporta computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de GPU Passthrough e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere e Hyper-V (somente passthrough).

Usando o GPU Passthrough, você pode criar VMs que têm acesso exclusivo a hardware de processamento gráfico dedicado. Você pode instalar várias GPUs no hipervisor e atribuir VMs a cada uma dessas GPUs em uma base um-para-um.

Usando a virtualização de GPU, várias máquinas virtuais podem acessar diretamente o poder de processamento gráfico de uma única GPU física.

### Aceleração de GPU para SO de múltiplas sessões do Windows

O HDX 3D Pro permite que aplicativos com muitos gráficos em execução em sessões do SO de múltiplas sessões do Windows sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor. Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

#### Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais compatível. Em vez disso, use Thinwire com transporte adaptável ativado.

> Framehawk é uma tecnologia de acesso remoto de exibição para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE). O Framehawk supera os desafios de interferência espectral e propagação multitrilha e oferece uma experiência de usuário fluida e interativa para usuários de aplicativos e desktops virtuais.

### Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e permitir o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você

pode especificar uma marca d'água que é uma camada de texto. A marca d'água pode ser exibida em toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte VDA.

### Taxa de Atualização Adaptável

Com as novas melhorias de escalabilidade, o HDX corresponde à taxa de atualização de monitores virtuais para corresponder à política de FPS de destino definida. A Taxa de Atualização Adaptável (ARR) está disponível para VDAs de sessão única e multissessão e funciona para cenários acelerados por GPU e não-GPU.

### modo tolerante a perdas

O modo tolerante a perdas foi completamente reformulado para garantir que a sessão permaneça interativa quando a perda de pacotes for detectada.

## Informações relacionadas

- HDX 3D Pro
- Aceleração de GPU para SO Windows de sessão única
- Aceleração de GPU para SO Windows de multissessão
- Framehawk
- Thinwire
- Marca d'água de sessão baseada em texto

## High Dynamic Range (HDR) de 10 bits

Com sessões de desktop virtual High Dynamic Range (HDR) de 10 bits, você pode usar recursos aprimorados de codificação e decodificação para renderizar imagens e vídeos de alta qualidade com uma gama estendida de cores e maior contraste e brilho. Além disso, você pode personalizar o nível de luminância branca, os Dados de Identificação de Tela Estendidos (EDID) e a qualidade visual para melhorar a experiência do usuário.

### Requisitos do sistema

Ponto de extremidade:

- Aplicativo Citrix Workspace™ para Windows 2209 ou posterior para GPUs NVIDIA

- GPUs NVIDIA com suporte para decodificação HEVC (H.265) 444 de 10 bits no ponto de extremidade
- Monitores com suporte a HDR de 10 bits, o HDR de 10 bits deve ser habilitado em todos os monitores usando as configurações de exibição.

Servidor:

- VDA de SO de sessão única do Windows 2209 ou posterior para GPUs NVIDIA, e VDA 2308 ou posterior para GPUs Intel
- GPUs NVIDIA com suporte para codificação HEVC 444 de 10 bits no VDA

## Políticas necessárias

Ponto de extremidade:

- Habilitar decodificação H.265 para gráficos

Servidor:

- Otimizar para carga de trabalho de gráficos 3D
- Indicador de Status Gráfico (opcional)

## Configurações do servidor

O lançamento de uma sessão Citrix® em um monitor de endpoint com HDR de 10 bits ativado habilita a sessão HDR por padrão. Em sessões HDR com vários monitores, todos os monitores de endpoint devem ter HDR de 10 bits ativado. As sessões HDR são suportadas nos modos de janela e tela cheia.

### Nível de Branco de Referência

Essa configuração define o nível de luminância branca pelo valor em nits. Ela controla o brilho relativo da tela HDR dentro da sessão. O valor padrão é 80 nits. Defina a seguinte chave de registro para definir um valor de nit diferente:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_DWORD
- Name: RefWhiteLevel

Para ativar a configuração, você deve redimensionar sua sessão ou desconectar e reiniciar a sessão.

### Substituição de EDID

Você pode configurar o VDA para usar o EDID do monitor de endpoint para suas sessões HDR. Isso permite que você utilize totalmente os recursos de exibição do monitor, combinando a gama de cores e o intervalo de luminância. Por padrão, as sessões HDR assumem um monitor compatível com HDR1000. Você pode exportar o EDID do monitor de endpoint usando NVIDIA ou outras ferramentas. Aplique-o ao VDA usando a seguinte chave de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_BINARY
- Name: EDIDOverride

Ao armazenar o EDID no registro, ele não deve conter vírgulas, espaços ou caracteres especiais. Para ativar a substituição de EDID, saia e inicie uma nova sessão.

### Experiência visual sem perdas

Habilite as seguintes políticas para uma experiência visualmente sem perdas:

- Permitir Compressão Visual Sem Perdas
- Qualidade Visual: Sempre Sem Perdas ou Construir para Sem Perdas

Depois que as políticas forem definidas, você pode controlar a qualidade da sessão HDR usando o Indicador de Status Gráfico, usando o Controle Deslizante de Qualidade da Imagem ou alternando para o modo pixel-perfect.

### Permitir bloqueio de tela do Windows

Você pode usar esta política para permitir que todos os tempos limite de exibição do Windows, incluindo o bloqueio de tela, se apliquem a uma sessão de Citrix Virtual Desktop em um SO de Estação de Trabalho. Essa configuração pode ser definida usando um Objeto de Política de Grupo do Citrix no Citrix Studio.

Por padrão, quando essa configuração não está habilitada, um Citrix Virtual Desktop não responde a tempos limite para bloqueio de sessão, protetor de tela ou desligamento da tela, durante uma sessão ativa.

Quando um protetor de tela protegido por senha é configurado em um VDA de Estação de Trabalho, essa configuração deve ser habilitada para permitir que a sessão do Citrix Virtual Desktop seja bloqueada automaticamente quando o tempo limite do protetor de tela for atingido.

Habilitar essa configuração quando um tempo limite de desligamento da tela é configurado no VDA faz com que a expiração desse tempo limite resulte em uma sessão que não é atualizada até que o usuário retome a interação com a sessão. Por exemplo, qualquer tempo exibido não é atualizado e novas notificações não são exibidas.

### Outras considerações

- Você pode iniciar sessões HDR de 10 bits em até quatro monitores em GPUs virtuais.
- A sessão do Citrix reverte para um modo de 8 bits, não-HDR, nas seguintes instâncias:
  - Se quaisquer monitores de endpoint não tiverem HDR de 10 bits habilitado
  - Habilitar o compartilhamento de tela.
  - Definir um layout de exibição virtual no VDA.
  - Alternar para o modo pixel-perfect sem definir a política **Permitir Compressão Visualmente Sem Perdas**.

## HDX™ 3D Pro

Os recursos HDX 3D Pro do Citrix Virtual Apps and Desktops™ permitem que você forneça desktops e aplicativos que apresentam o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta a aceleração de GPU apenas para DirectX.

Para as configurações de política do HDX 3D Pro, consulte Otimizar para carga de trabalho de gráficos 3D.

Todos os aplicativos Citrix Workspace compatíveis podem ser usados com gráficos 3D. Para obter o melhor desempenho com cargas de trabalho 3D complexas, monitores de alta resolução, configurações de vários monitores e aplicativos de alta taxa de quadros, recomendamos as versões mais recentes do Citrix Workspace app para Windows e do Citrix Workspace app para Linux. Para obter mais informações sobre as versões compatíveis do Citrix Workspace app, consulte Marcos do ciclo de vida do Citrix Workspace app.

Exemplos de aplicativos profissionais 3D incluem:

- Aplicativos de design, fabricação e engenharia assistidos por computador (CAD/CAM/CAE)
- Software de Sistema de Informação Geográfica (GIS)
- Sistema de Comunicação e Arquivamento de Imagens (PACS) para imagens médicas

- Aplicativos que usam as versões mais recentes de OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL
- Aplicativos não gráficos computacionalmente intensivos que usam GPUs NVIDIA Compute Unified Device Architecture (CUDA) para computação paralela

O HDX 3D Pro oferece a melhor experiência do usuário em qualquer largura de banda:

- Em conexões WAN: Ofereça uma experiência de usuário interativa em conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de um desktop local em conexões LAN.

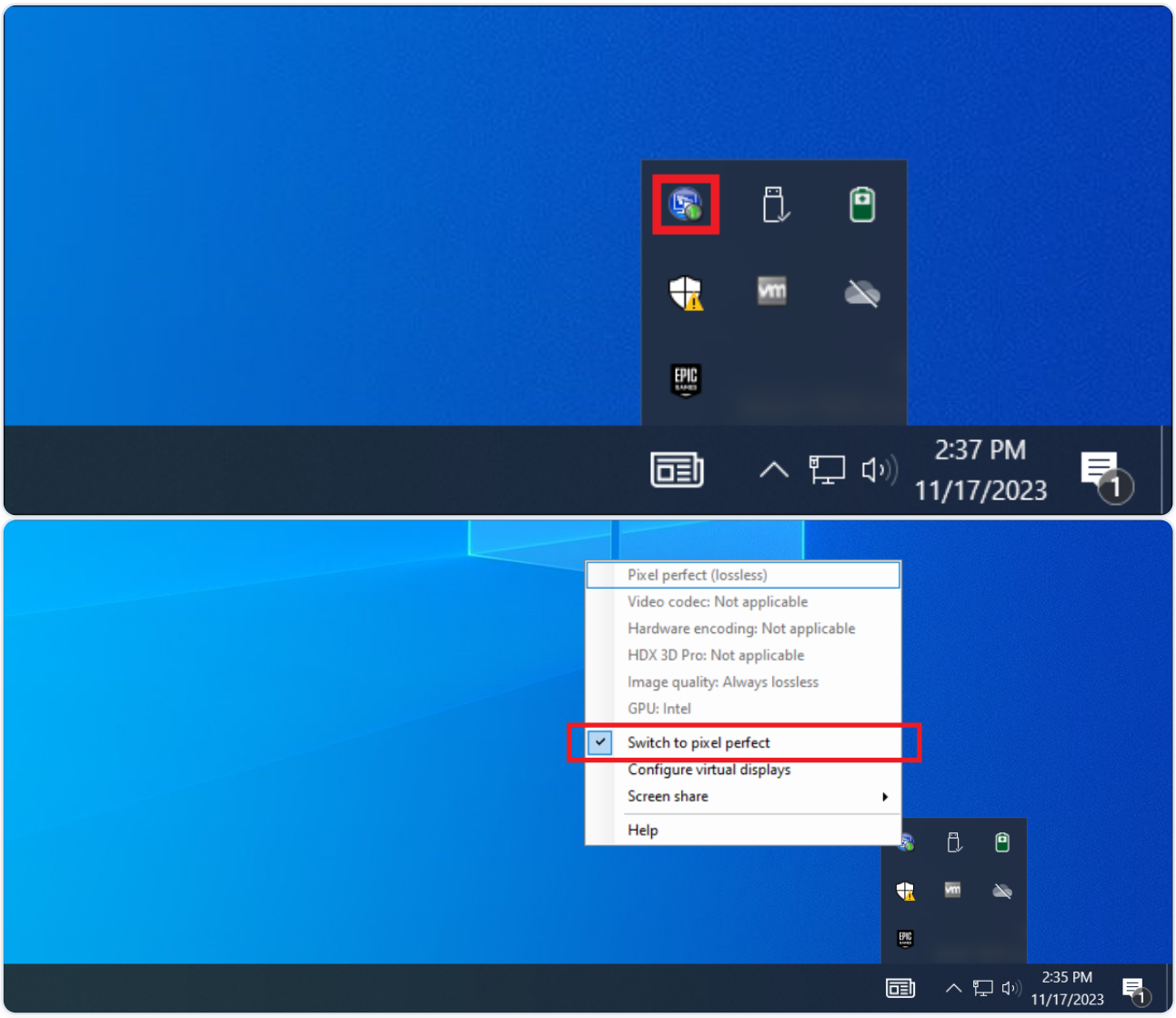
  Você pode substituir estações de trabalho complexas e caras por dispositivos de usuário mais simples, movendo o processamento gráfico para o data center para gerenciamento centralizado.

## Opção de compactação sem perdas para casos de uso especializados

O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixels são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

Ao usar a compressão sem perdas:

- O indicador sem perdas no Indicador de Status Gráfico, um ícone na área de notificação, notifica o usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração da política de **Qualidade Visual** especifica **Construir para sem perdas**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.




- O switch sem perdas permite ao usuário mudar para o modo **Sempre Sem Perdas** a qualquer momento dentro da sessão. Para selecionar ou desmarcar **Sem Perdas** dentro de uma sessão, clique com o botão direito do mouse no ícone e clique em **Mudar para pixel perfeito** ou use o atalho ALT+SHIFT+1.
    - Para compressão sem perdas: O HDX 3D Pro usa o codec sem perdas para compressão, independentemente do codec selecionado por meio da política.
    - Para compressão com perdas: O HDX 3D Pro usa o codec original, seja o padrão ou o selecionado através da política. As configurações do switch sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Sempre sem perdas** na configuração da política de **qualidade visual**.

Você pode substituir o atalho padrão, ALT+SHIFT+1, para selecionar ou desmarcar Sem Perdas dentro de uma sessão. Configure uma nova configuração de registro em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

- Nome: HKEY_LOCAL_MACHINE_HotKey, Tipo: String
- O formato para configurar uma combinação de atalho é C=0|1, A=0|1, S=0|1, W=0|1, K=val. As chaves devem ser separadas por vírgula “,”. A ordem das chaves não importa.
- A, C, S, W e K são chaves, onde C=Control, A=ALT, S=SHIFT, W=Win, e K=uma chave válida. Os valores permitidos para K são 0–9, a–z e qualquer código de chave virtual.
- Por exemplo: Para F10, defina K=0x79 Para Ctrl + F10, defina C=1, K=0x79 Para Alt + A, defina A=1, K=a ou A=1, K=A ou K=A, A=1 Para Ctrl + Alt + 5, defina C=1, A=1, K=5 ou A=1, K=5, C=1 Para Ctrl + Shift + F5, defina A=1, S=1, K=0x74

## Otimizar a experiência do usuário do HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política de limite de largura de banda geral da sessão para limitar a capacidade disponível para cada usuário. O uso dessa configuração garante que a capacidade disponível não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações nesta ao longo das sessões dos usuários podem impactar negativamente o desempenho. Por exemplo, se 20 usuários compartilham uma conexão de 60 Mbps, a capacidade disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a capacidade necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre. Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo CTX128190 da Central de Conhecimento. Use a ferramenta HDX Monitor para validar a operação e a configuração das tecnologias de visualização HDX e para diagnosticar e solucionar problemas do HDX. A ferramenta está disponível na pasta **Support** na mídia de instalação do Citrix Virtual Apps and Desktops.

## Aceleração de GPU para SO Windows multi-sessão

O Citrix Virtual Apps and Desktops™ oferece suporte a aplicativos com muitos gráficos executados em sessões do SO Windows Multi-sessão para renderizar na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a CPU do servidor pode ser usada com mais eficiência.

Como o Windows Server é um sistema operacional multiusuário, vários usuários podem compartilhar uma GPU acessada pelo Citrix Virtual Apps™ sem a necessidade de virtualização de GPU (vGPU).

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

### Compartilhamento de GPU

O Compartilhamento de GPU permite a renderização de hardware de GPU de aplicativos OpenGL e DirectX em sessões de área de trabalho remota. Ele possui as seguintes características:

- Pode ser usado em máquinas bare metal ou virtuais para aumentar a escalabilidade e o desempenho do aplicativo.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não exige o desempenho de renderização de uma GPU dedicada).
- Não requer configurações especiais.

Uma GPU pode ser atribuída à máquina virtual do Windows Server nos modos de pass-through completo ou GPU virtual (vGPU), seguindo os requisitos do Hypervisor e do fornecedor da GPU. Implantações bare-metal em máquinas físicas do Windows Server também são suportadas.

O Compartilhamento de GPU não depende de nenhuma placa gráfica específica.

- Para máquinas virtuais, selecione uma placa gráfica compatível com o Hypervisor em uso. Para uma lista de compatibilidade de hardware do XenServer, consulte Lista de Compatibilidade de Hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de vídeo habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desabilite todas, exceto uma, usando o Gerenciador de Dispositivos.

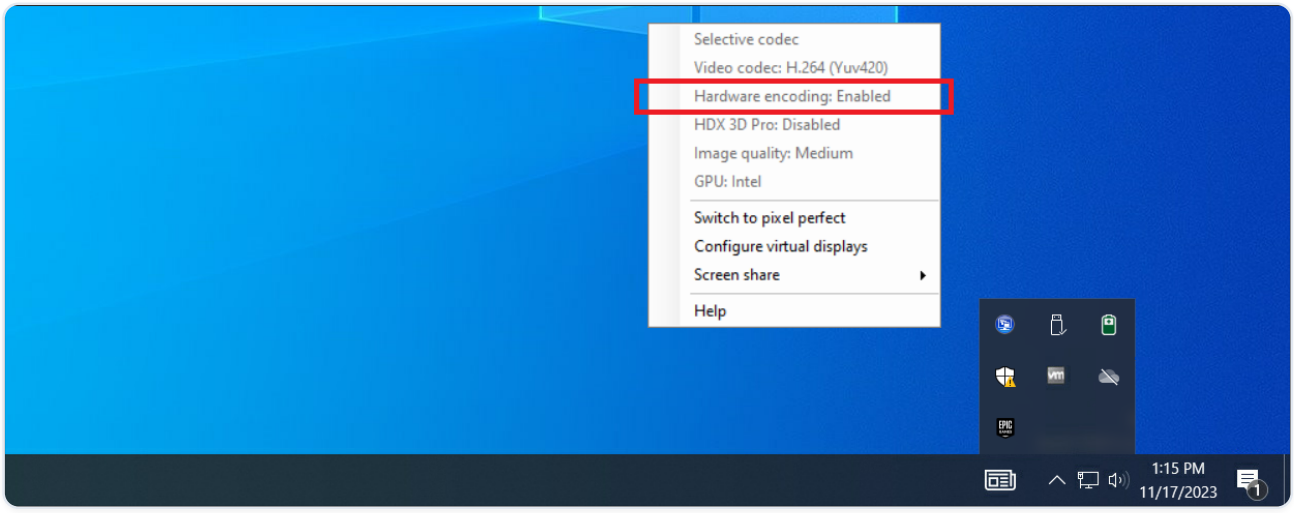
A escalabilidade usando o Compartilhamento de GPU depende de vários fatores:

- Os aplicativos em execução
- A quantidade de RAM de vídeo que eles consomem
- O poder de processamento da placa gráfica

Alguns aplicativos manipular a escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha do driver da placa gráfica. Limite o número de usuários simultâneos para evitar tais problemas.

- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso e permite o uso de codificação de hardware para codificação H.264 (onde disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política gráfica.

Para confirmar que a aceleração da GPU está ocorrendo, o Indicador de Status Gráfico pode ser usado:




### Renderização DirectX, Direct3D e WPF

A renderização DirectX, Direct3D e WPF está disponível apenas em servidores com uma GPU que suporte uma interface de driver de vídeo (DDI) versão 9ex, 10 ou 11.

- No Windows Server 2016 e posterior, as sessões dos Serviços de Área de Trabalho Remota (RDS) no servidor Host da Sessão RD usam o Driver de Renderização Básico da Microsoft como adaptador padrão. Para usar a GPU em sessões RDS no Windows Server 2016 e posterior, habilite a configuração **Usar o adaptador gráfico padrão de hardware para todas as sessões dos Serviços de Área de Trabalho Remota** na política de grupo **Política de Computador Local** \> **Configuração do Computador** \> **Modelos Administrativos** \> **Componentes do Windows** \> **Serviços de Área de Trabalho Remota** \> **Host da Sessão da Área de Trabalho Remota** \> **Ambiente de Sessão Remota**.
- Para permitir que aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no registro do servidor que executa sessões do SO Windows Multi-sessão. Para

obter informações sobre a configuração do registro, consulte Renderização do Windows Presentation Foundation (WPF) na lista de recursos gerenciados através do registro.

### Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos de aceleração CUDA, habilite as configurações do registro. Para obter informações, consulte Aceleração de GPU para aplicativos CUDA ou OpenCL na lista de recursos gerenciados através do registro.

## Aceleração de GPU para SO de sessão única do Windows

Com o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de desktops hospedados ou aplicativos em máquinas de SO de sessão única. O HDX 3D Pro oferece suporte a computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de Passthrough de GPU e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere, Nutanix e Hyper-V (somente passthrough).

O HDX™ 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para desempenho ideal de WAN e sem fio. O HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que suportam NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que suportam NVENC.
- Opção de compressão sem perdas para casos de uso especializados. O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixels são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

**Cuidado:**

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

- Suporte a vários monitores e monitores de alta resolução. Para máquinas de SO de sessão única, são suportados até 8 monitores 4K. Os usuários podem organizar seus monitores em qualquer configuração e podem misturar monitores com diferentes resoluções e orientações. O número de monitores é limitado pelas capacidades da GPU do computador host, do dispositivo do usuário e da largura de banda disponível. O HDX 3D Pro suporta todas as resoluções de monitor e é limitado apenas pelas capacidades da GPU no computador host.
- Resolução dinâmica. Você pode redimensionar a área de trabalho virtual ou a janela do aplicativo para qualquer resolução. **Nota:** O único método suportado para alterar a resolução é redimensionar a janela da sessão VDA. Alterar a resolução de dentro da sessão VDA (usando **Painel de Controle > Aparência** e **Personalização > Vídeo > Resolução da Tela) não é suportado**.
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro oferece suporte a placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passthrough de GPU e compartilhamento de GPU. O NVIDIA vGPU permite que várias VMs tenham acesso simultâneo e direto a uma única GPU física, usando os mesmos drivers gráficos NVIDIA que são implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar o HDX 3D Pro com vDGA para cargas de trabalho RDS e VDI.
- Suporte para VMware vSphere/ESX.
- Suporte para Microsoft HyperV usando Atribuição de Dispositivo Discreto no Windows Server 2016.
- Suporte para Data Center Graphics com a família de processadores Intel Xeon E3 e a série Intel Data Center GPU Flex. Para obter mais informações, consulte `<https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`.
- Suporte para GPUs AMD.

> Nota:
>
> O suporte para AMD MxGPU (virtualização de GPU) funciona apenas com vGPUs VMware vSphere. O Citrix Hypervisor e o Hyper-V são suportados com passthrough de GPU. Para obter mais informações, consulte `<https://www.amd.com/en/graphics/workstation-virtual-graphics>`.

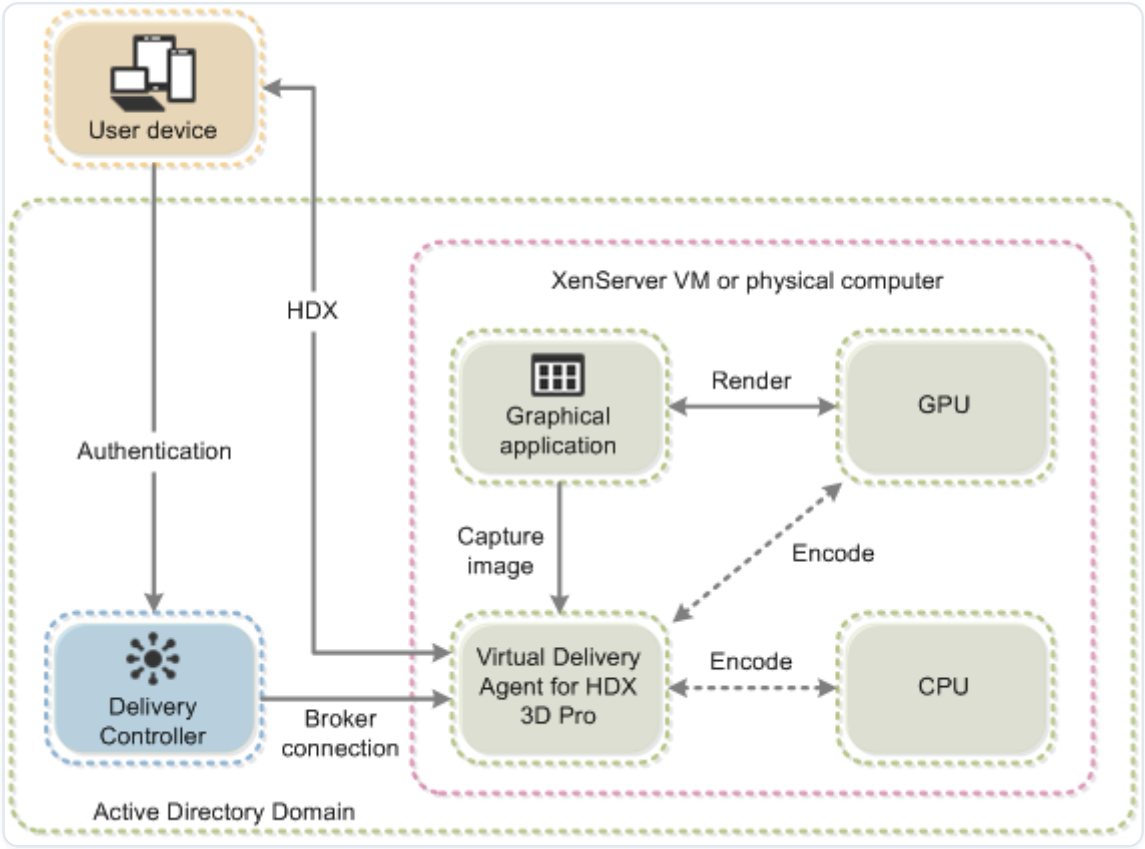
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e GPUs Intel. Uma configuração de política (habilitada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para H.264, H.265 ou codificação AV1 (onde disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política gráfica.

Conforme mostrado na figura a seguir:

- Quando um usuário faz login no aplicativo Citrix Workspace™ e acessa o aplicativo ou área de trabalho virtual, o Controller autentica o usuário. O Controller então entra em contato com o VDA para HDX 3D Pro para intermediar uma conexão com o computador que hospeda o aplicativo gráfico.

O VDA para HDX 3D Pro usa o hardware apropriado no host para compactar visualizações do desktop completo ou apenas do aplicativo gráfico.

- As visualizações do desktop ou aplicativo e as interações do usuário com eles são transmitidas entre o computador host e o dispositivo do usuário. Essa transmissão é feita por meio de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



### Otimizar a experiência do usuário do HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política **Limite geral de largura de banda da sessão** para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que a largura de banda disponível não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações na largura de banda disponível ao longo das sessões do usuário podem impactar negativamente o desempenho.

Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a largura de banda necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre.

Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo do Knowledge Center CTX128190.

### Compressão sem perdas

Ao usar a compressão sem perdas:

- O indicador sem perdas, um ícone na área de notificação, notifica o usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração da política de **Qualidade Visual** especifica **Construir para sem perdas**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.
- O switch sem perdas permite ao usuário mudar para o modo **Sempre sem perdas** a qualquer momento dentro da sessão. Para selecionar ou desmarcar Sem perdas a qualquer momento dentro de uma sessão, clique com o botão direito do mouse no ícone e clique em **Mudar para pixel perfeito** ou use o atalho **ALT+SHIFT+1**.
- Para compressão sem perdas: O HDX 3D Pro usa o codec sem perdas para compressão, independentemente do codec selecionado por meio da política.
- Para compressão com perdas: O HDX 3D Pro usa o codec original, seja o padrão ou o selecionado por meio da política.
- As configurações do switch sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Sempre sem perdas** na configuração da política de **Qualidade visual**.

### Tecla de atalho sem perdas

Você pode usar uma tecla de atalho para selecionar ou desmarcar **Sem perdas** a qualquer momento dentro de uma sessão, usando o atalho padrão **ALT+SHIFT+1**.

Você pode substituir o atalho padrão, **ALT+SHIFT+1**, no Registro do Windows. Para configurar uma nova configuração de Registro, defina os seguintes valores de registro:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **Nome**: `HKLM_HotKey`
- **Tipo**: `String`

O formato para configurar uma combinação de atalho é `C=0|1, A=0|1, S=0|1, W=0|1, K=val`. As chaves devem ser separadas por vírgula “,” sem espaço. A ordem das chaves não importa.

A, C, S, W e K são chaves, onde C=Control, A=ALT, S=SHIFT, W=Win, e K=uma chave válida onde os valores permitidos para K são 0–9, a–z e qualquer código de tecla virtual.

Por exemplo,

- Para **F10**, defina K=0x79
- Para **Ctrl + F10**, defina C=1, K=0x79
- Para **Alt + A**, defina A=1,K=a ou A=1,K=A ou K=A,A=1
- Para **Ctrl + Alt + 5**, defina C=1, A=1,K=5 ou A=1,K=5,C=1
- Para **Ctrl + Shift + F5**, defina A=1,S=1,K=0x74

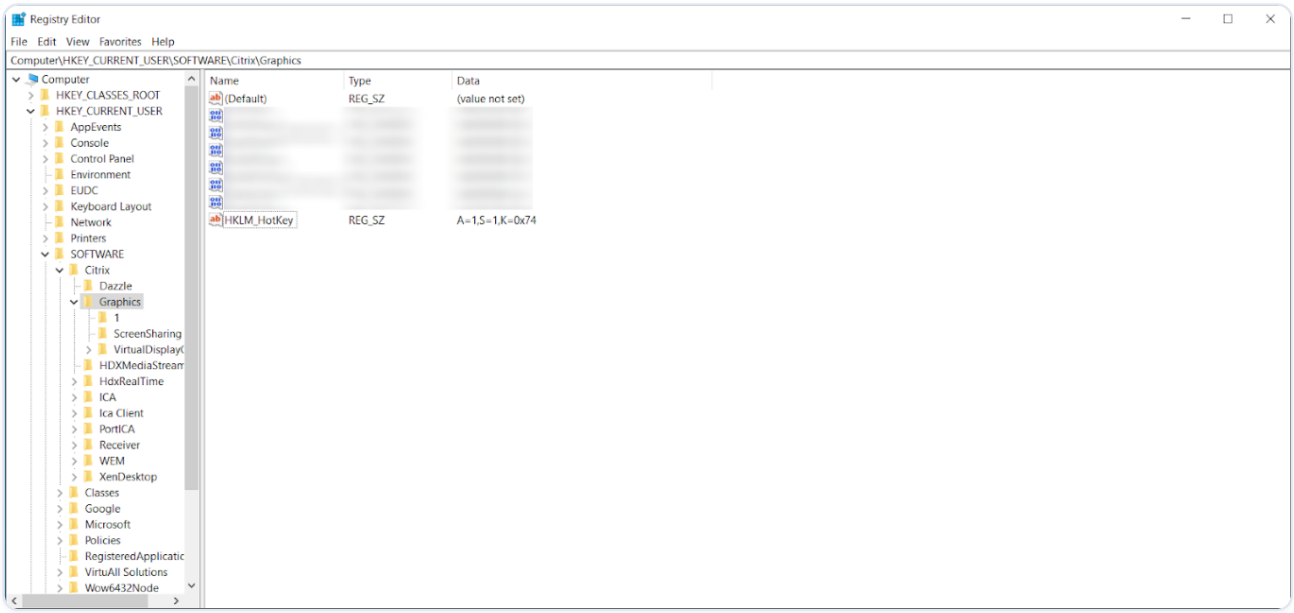
A tabela a seguir mostra a lista de exemplo de códigos de tecla virtual:

| CHAVE | VALOR |
|---|---|
| F1 | 0x70 |
| F2 | 0x71 |
| F3 | 0x72 |
| F4 | 0x73 |
| F5 | 0x74 |

| CHAVE | VALOR |
|---|---|
| F6 | 0x75 |
| F7 | 0x76 |
| F8 | 0x77 |
| F9 | 0x78 |
| F10 | 0x79 |
| F11 | 0x7A |
| F12 | 0x7B |
| Tecla PAGE UP | 0x21 |
| Tecla PAGE DOWN | 0x22 |
| Tecla END | 0x23 |
| Tecla HOME | 0x24 |
| Tecla SETA PARA A ESQUERDA | 0x25 |
| Tecla SETA PARA CIMA | 0x26 |
| Tecla SETA PARA A DIREITA | 0x27 |
| Tecla SETA PARA BAIXO | 0x28 |

Certifique-se de que não há espaço entre as combinações de atalho. Por exemplo:

Correto: C=1,K=0x74 Incorreto: C=1, K=0x74




**Cuidado:**

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

# Thinwire

## Introdução

Thinwire, uma parte da tecnologia Citrix HDX, é a tecnologia de remotização de exibição padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de remotização de exibição permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição.

Uma solução de remotização de exibição bem-sucedida oferece uma experiência de usuário altamente interativa, semelhante à de um PC local. O Thinwire alcança essa experiência usando uma variedade de técnicas complexas e eficientes de análise e compressão de imagem. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de remotização de exibição.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso de negócios gerais e é usado como a tecnologia de remotização de exibição padrão no Citrix Virtual Apps and Desktops.

## HDX™ 3D Pro

Em sua configuração padrão, o Thinwire pode fornecer gráficos 3D ou altamente interativos e usar uma unidade de processamento gráfico (GPU), se presente. No entanto, recomendamos habilitar o modo HDX 3D Pro usando as políticas **Otimizar para carga de trabalho de gráficos 3D** ou **Qualidade visual > Construir para sem perdas** para cenários em que GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264, H.265 ou AV1) para codificar a tela inteira usando aceleração de hardware, se uma GPU estiver presente. Isso proporciona uma experiência mais fluida para gráficos profissionais 3D. Para obter mais informações, consulte H.264 Build to lossless, HDX 3D Pro e Aceleração de GPU para SO de sessão única do Windows.

## Requisitos

O Thinwire é otimizado para sistemas operacionais modernos, incluindo Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 e Windows 7. Para Windows Server 2008 R2, o modo gráfico legado é recomendado. Use os modelos de política Citrix integrados, Alta Escalabilidade de Servidor - SO Legado e Otimizado para WAN - SO Legado para fornecer as combinações recomendadas pela Citrix das configurações de política para esses casos de uso.

- A configuração de política que impulsiona o comportamento do Thinwire - **Usar codec de vídeo para compressão** está disponível nas versões VDA do Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp and XenDesktop 7.6 FP3 e posterior. A opção **Usar codec de vídeo quando preferencial** é a configuração padrão nas versões VDA do Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp and XenDesktop 7.9 e posterior.
- Todos os aplicativos Citrix Workspace™ suportam Thinwire. Alguns aplicativos Citrix Workspace podem suportar recursos do Thinwire que outros não, por exemplo, gráficos de 8 bits ou 16 bits para uso reduzido de largura de banda. O suporte para tais recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos do servidor (CPU, memória) em cenários de múltiplos monitores e alta resolução. É possível ajustar a quantidade de recursos que o Thinwire usa, no entanto, o uso da largura de banda pode aumentar como resultado.
- Em cenários de baixa largura de banda ou alta latência, considere habilitar gráficos de 8 bits ou 16 bits para melhorar a interatividade. A qualidade visual pode ser afetada, especialmente em profundidade de cor de 8 bits.

## Métodos de codificação

Thinwire pode operar em dois modos de codificação diferentes, dependendo da política e dos recursos do cliente:

- Thinwire com JPEG Adaptativo Configuração da política **Usar codec de vídeo para compactação**: **Não usar codec de vídeo**
- Thinwire com H.264, H.265 ou AV1 Seletivo Configuração da política **Usar codec de vídeo para compactação**: **Usar codec de vídeo quando preferencial** ou **Para regiões em mudança ativa**
- Thinwire com H.264, H.265 ou AV1 em Tela Cheia Configuração da política **Usar codec de vídeo para compactação**: **Para a tela inteira**

## H.265

High Efficiency Video Coding (HEVC), também conhecido como H.265, é o sucessor do H.264. A codificação de hardware com o codec de vídeo H.265 é suportada nas seguintes GPUs:

- GPUs NVIDIA baseadas em Maxwell e superiores
- GPUs Intel de 6ª geração e superiores
- GPUs AMD baseadas em Raven e superiores

## AV1

A Citrix adicionou suporte para o codec de vídeo AV1. O benefício do AV1 é que ele possui compactação de imagem superior, melhor qualidade de imagem e menor uso de largura de banda em comparação com H.264 e H.265.

Os seguintes requisitos para AV1 devem ser atendidos:

- VDA 2305 ou superior para GPUs NVIDIA, ou
- VDA 2308 ou superior para GPUs Intel

As seguintes GPUs são compatíveis para codificação:

- GPU NVIDIA baseada em Ada Lovelace
- GPUs Intel ARC ou Intel Data Center GPU Flex Series

Para mais informações sobre as GPUs Ada Lovelace da NVIDIA, consulte arquitetura ADA.

Para mais informações sobre as GPUs Flex Series para estações de trabalho e data centers ARC da Intel, consulte série Flex e Visão geral.

## Seleção automática de codec de vídeo

Você pode detectar automaticamente o melhor codec de vídeo a ser usado quando a política **Usar codec de vídeo** para compactação estiver habilitada ou Otimizar para carga de trabalho de gráficos 3D estiver habilitada no VDA. Durante a instalação do aplicativo Citrix Workspace para Windows, as capacidades de decodificação do endpoint são avaliadas. Com base nessas informações, o aplicativo Citrix Workspace para Windows negocia o melhor codec a ser usado com o VDA na conexão. A lista a seguir descreve a ordem em que os codecs de vídeo são avaliados:

- AV1
- H.265
- H.264

A seleção automática se aplica apenas às variantes 4:2:0 desses codecs. Se a configuração **Qualidade Visual** estiver definida como 'Build-to-Lossless' ou 'Always Lossless' e quando Permitir Visualmente Sem Perdas estiver definida como 'habilitado', a seleção automática do codec de vídeo é desabilitada.

Ao se conectar a um recurso, o aplicativo Citrix Workspace testa a capacidade do endpoint de decodificar H.265 e AV1 e salva as capacidades no registro. O aplicativo Citrix Workspace então seleciona automaticamente o melhor codec de vídeo a ser usado e negocia isso com o VDA. Se tanto o VDA quanto o cliente puderem usar H.265 e AV1, então AV1 será selecionado como o codec de vídeo. Se AV1 não estiver disponível no VDA ou no cliente, H.265 é negociado. Se H.265 também não estiver disponível em nenhum dos dois, a sessão usa H.264 como o codec de vídeo.

> **Observação:**
>
> Este recurso está ativado por padrão. Esse comportamento pode ser alterado definindo a nova configuração de registro do lado do cliente `DisableDecoderCaps`.
>
> Para desabilitar a seleção automática do codec de vídeo, defina 'DisableDecoderCaps' como `HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD`

> `DisableDecoderCaps = 1` ou `HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`.

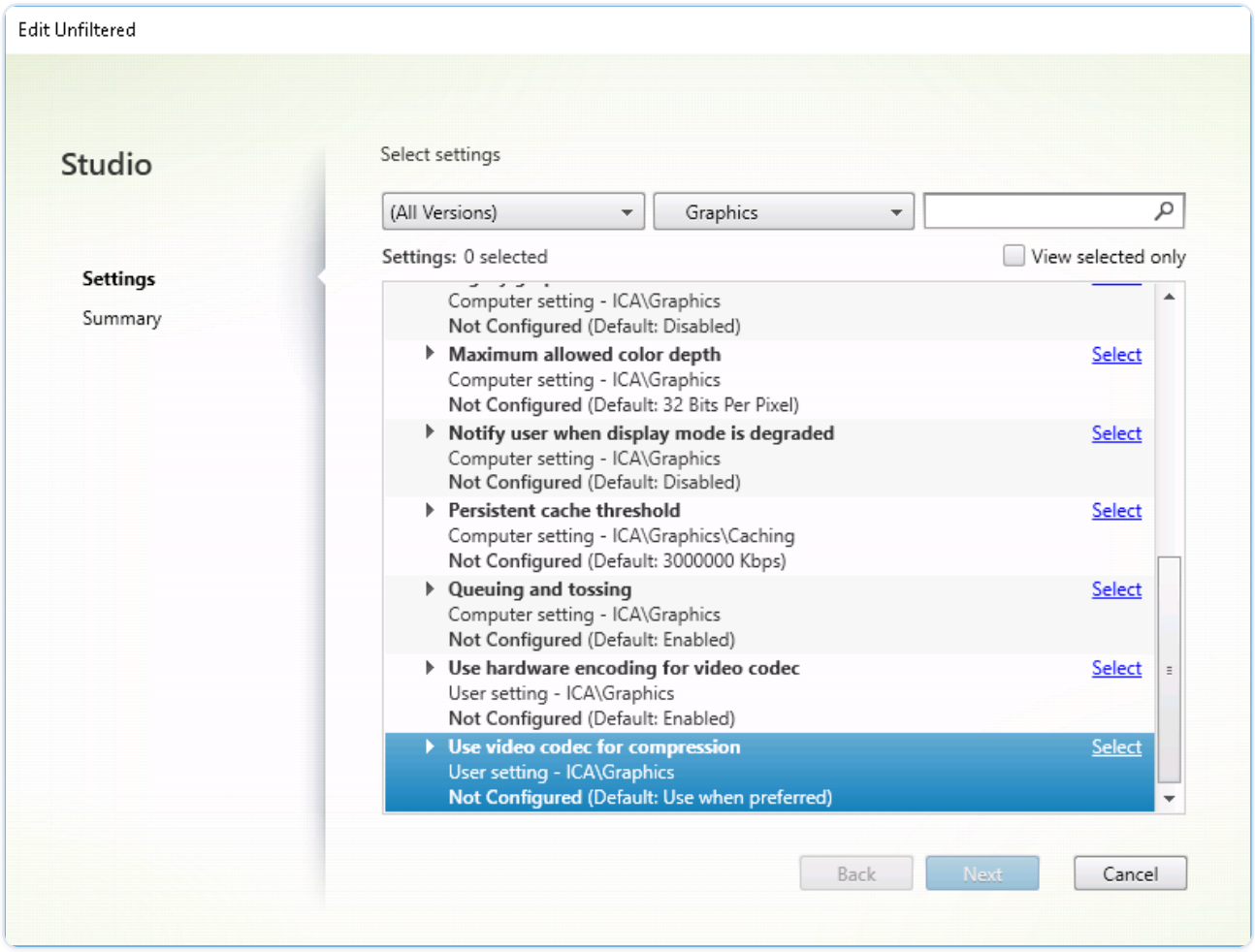
Se qualquer um desses valores for definido como 1, a seleção automática do codec de vídeo não será usada. O indicador de status gráfico e o monitor HDX podem monitorar o codec de vídeo.

## Configuração

Thinwire é a tecnologia padrão de exibição remota.

A seguinte configuração de política de Gráficos define o padrão e oferece alternativas para diferentes casos de uso:

- Usar codec de vídeo para compactação
  - **Usar codec de vídeo quando preferencial**. Esta é a configuração padrão. Nenhuma configuração adicional é necessária. Manter esta configuração como padrão garante que o Thinwire seja selecionado para todas as conexões Citrix e seja otimizado para escalabilidade, largura de banda e qualidade de imagem superior para cargas de trabalho típicas de desktop. Isso é funcionalmente equivalente a **Para regiões em mudança ativa**.
- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:
  - **Para regiões em mudança ativa**. A tecnologia de exibição adaptativa no Thinwire identifica imagens em movimento (vídeo, 3D em movimento) e usa H.264, H.265 ou AV1 apenas na parte da tela onde a imagem está se movendo.
  - **Para a tela inteira**. Oferece Thinwire em tela cheia com H.264, H.265 ou AV1 para otimizar a experiência do usuário e a largura de banda em casos de uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visualmente sem perdas** está desabilitada), a imagem final não é perfeita em pixels (sem perdas) e pode não ser adequada para certos cenários. Nesses casos, considere usar H.264 Build to lossless ou H.265 Build to lossless.




Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de exibição remota. O Thinwire as suporta todas.

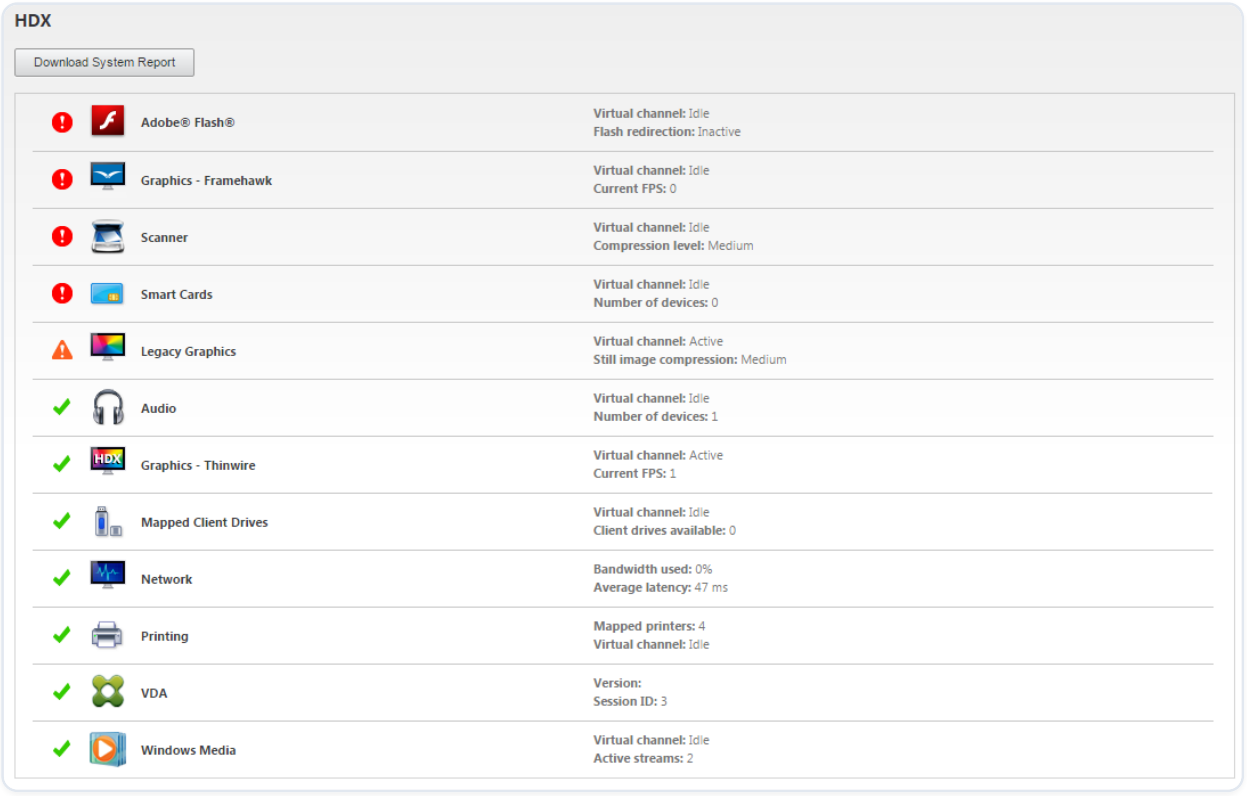
- Profundidade de cor preferida para gráficos simples
- Taxa de quadros alvo
- Qualidade visual

Para obter as combinações recomendadas pela Citrix de configurações de política para diferentes casos de uso de negócios, use os modelos de política Citrix integrados. Os modelos **Alta Escalabilidade de Servidor** e **Experiência de Usuário de Altíssima Definição** usam Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos seus usuários.

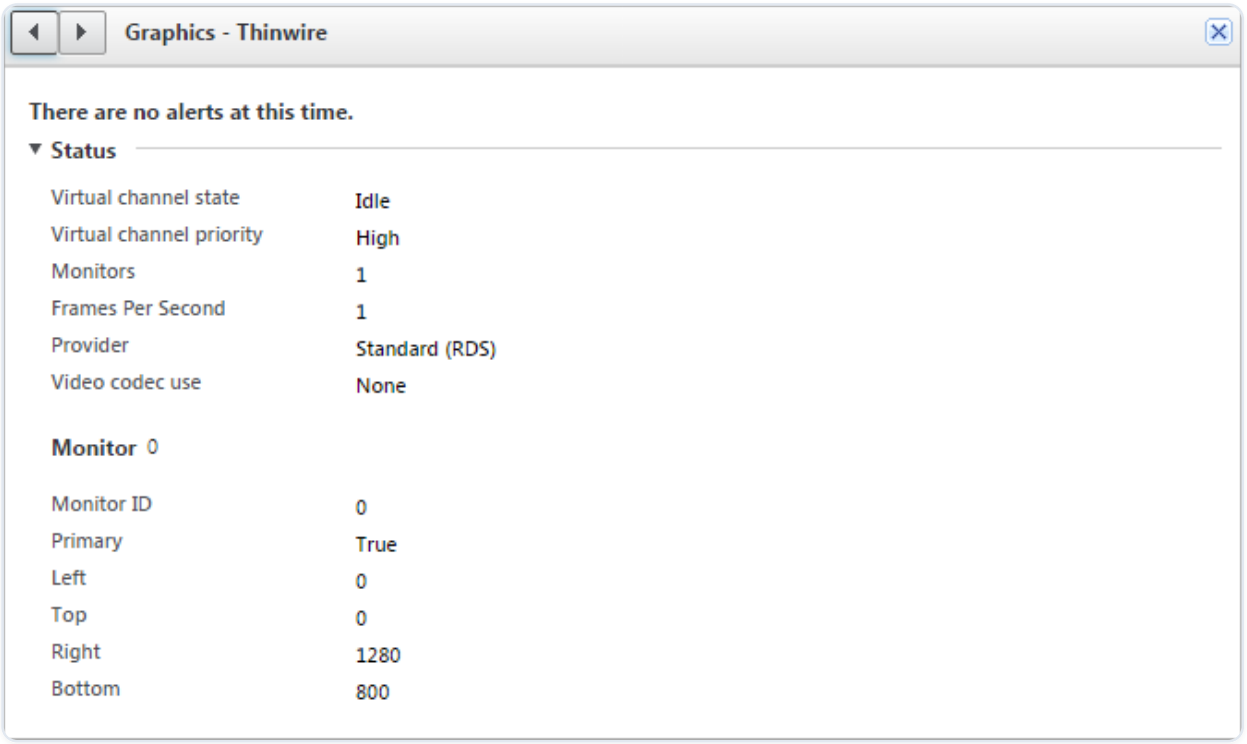
## Monitorando o Thinwire

Você pode monitorar o uso e o desempenho do Thinwire a partir do Citrix Director. A exibição de detalhes do canal virtual HDX contém informações úteis para solucionar problemas e monitorar o Thinwire em qualquer sessão. Para visualizar métricas relacionadas ao Thinwire:

1. No Director, procure por um usuário, máquina ou endpoint, abra uma sessão ativa e clique em **Detalhes**. Ou, você pode selecionar **Filtros** > **Sessões** > **Todas as Sessões**, abrir uma sessão ativa e clicar em **Detalhes**.
2. Role para baixo até o painel **HDX**.




3. Selecione **Graphics - Thinwire**.



## Codec de compressão sem perdas (MDRLE)

Em uma sessão de desktop típica, a maior parte das imagens são gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas usando o codec 2DRLE. No lado do cliente do aplicativo Citrix Workspace, esses elementos são decodificados usando o decodificador 2DRLE do lado do aplicativo Citrix Workspace para exibição da sessão.

No XenApp e XenDesktop 7.17, adicionamos um codec MDRLE com uma taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este novo codec não afeta a escalabilidade do servidor.

Menor largura de banda geralmente significa melhor interatividade da sessão (especialmente em links compartilhados ou restritos) e custos reduzidos.

A configuração não é necessária para o codec MDRLE. Se o aplicativo Citrix Workspace suportar a decodificação MDRLE, o VDA usa a codificação MDRLE do VDA e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA automaticamente retorna à codificação 2DRLE.

**Requisitos do MDRLE:**

- Citrix Virtual Apps and Desktops versão mínima 7 1808 VDAs
- XenApp e XenDesktop versão mínima 7.17 VDAs
- Citrix Workspace app para Windows versão mínima 1808
- Citrix Receiver para Windows versão mínima 4.11

## Modo Progressivo

O Citrix Virtual Apps and Desktops 1808 introduziu o modo progressivo e o ativou por padrão. Em condições de rede restritas (padrão: largura de banda < 2 Mbps, ou latência > 200 ms), o Thinwire aumentou a compressão de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens fortemente compactados são então progressivamente aprimorados, de forma aleatória em blocos, quando a atividade da tela para. Embora compactar e aprimorar dessa forma melhore a interatividade geral, isso reduz a eficiência do cache e aumenta o uso da largura de banda.

A partir do Citrix Virtual Apps and Desktops 1906, o modo progressivo está desativado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada nas condições da rede e varia entre um valor mínimo e máximo predefinido para cada configuração de **Qualidade visual**. Como não há uma etapa de aprimoramento explícita, o Thinwire otimiza a

entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

### Alterando o comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a chave do Registro. Para obter informações, consulte Modo progressivo na lista de recursos gerenciados por meio do Registro.

## Compilação para sem perdas

**Compilação para sem perdas** é uma configuração especial do Thinwire que otimiza a entrega de gráficos para interatividade e qualidade final da imagem. Você pode habilitar essa configuração definindo a política de **Qualidade visual** como **Compilação para sem perdas**.

A Compilação para sem perdas compacta a tela usando H.264, H.265 ou AV1 durante a atividade da tela e aprimora para pixel perfeito (sem perdas) quando a atividade para. A qualidade da imagem com perdas se adapta aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de aprimoramento é realizada gradualmente. Por exemplo, selecionar um modelo e girá-lo.

**Compilação para sem perdas** oferece todas as vantagens de usar um codec de vídeo para a tela inteira, incluindo aceleração de hardware, mas com o benefício adicional de uma tela final, garantidamente sem perdas. Isso é crítico para cargas de trabalho do tipo 3D que exigem uma imagem final perfeita em pixels. Por exemplo, manipular imagens médicas. Além disso, a **Compilação para sem perdas** H.264 usa menos recursos do que a tela cheia H.264 4:4:4. Como resultado, usar a **Compilação para sem perdas** geralmente resulta em uma taxa de quadros mais alta do que a H.264 4:4:4 visualmente sem perdas.

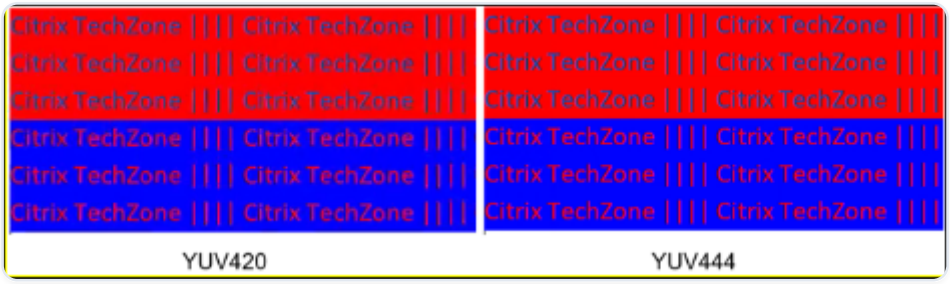
> **Observação:**
>
> Você pode desabilitar o uso de um codec de vídeo ao usar uma compilação para sem perdas. Basta definir a política **Usar codec de vídeo** como `Do not use video codec`. Isso resulta em imagens em movimento sendo codificadas com JPEG Adaptativo em vez disso.

## Codificação visualmente sem perdas

A codificação visualmente sem perdas usa o espaço de cores YUV 4:4:4 em vez do espaço de cores YUV 4:2:0 com subamostragem de croma para compactação de codec de vídeo. Isso

garante que nenhuma informação de cor seja perdida durante a conversão do espaço de cores e, uma vez decodificada, é visualmente imperceptível da imagem RGB original.

Considere o seguinte exemplo. Se usar um codec de vídeo para compactar a tela inteira, a compactação de cores 4:2:0 pode degradar detalhes de alto contraste, como texto, tornando-os borrados e mais difíceis de ler. Em contraste, 4:4:4 preserva quase todas as informações de cor e não exibe nenhuma degradação visualmente perceptível.




Cargas de trabalho que exigem qualidade perfeita de pixel ou exibição de cores precisa podem se beneficiar da codificação Visualmente Sem Perdas.

A codificação Visualmente Sem Perdas está disponível com H.264 e H.265. A codificação H.264 4:4:4 é uma solução puramente baseada em software e, como resultado, pode haver um impacto significativo na utilização da CPU tanto no VDA quanto no cliente. Isso também pode afetar a taxa de quadros.

O suporte a H.265 4:4:4 foi adicionado com o lançamento do Citrix Workspace app 2305, permitindo que o Thinwire use uma GPU no VDA e no cliente para codificação H.265 4:4:4, melhorando significativamente o desempenho.

Para permitir a codificação Visualmente Sem Perdas 4:4:4, duas políticas precisam ser habilitadas:

- **Qualidade Visual**: Definir como `Build to Lossless` ou `Always Lossless`
- **Permitir Sem Perdas Visuais**: Definir como `Enabled`

> **Observação:**
>
> Se **Permitir Sem Perdas Visuais** não estiver habilitado, mudamos para nosso codificador Thinwire em `Build to lossless` ou `Always Lossless`.

> H.265 4:4:4 sem perdas visuais tem os requisitos adicionais:

- GPUs NVIDIA exigem VDA versão 2209 ou superior

- GPUs Intel exigem VDA versão 2308 ou superior

As seguintes GPUs são compatíveis com H.265 4:4:4:

- GPUs NVIDIA de geração Pascal e posteriores
- GPUs Intel de 10ª geração e posteriores

Para o cliente, o aplicativo Citrix Workspace para Windows versão 2305 é necessária (a versão 2309.1 é recomendada).

A decodificação de hardware de H.265 4:4:4 é possível com as seguintes GPUs de dispositivo cliente:

- GPUs NVIDIA de geração Turing e posteriores
- GPUs Intel de 10ª geração e posteriores

## Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e permitem o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que é uma camada de texto, que é exibida sobre toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte de VDA.

> **Importante:**
>
> A marca d'água de sessão baseada em texto não é um recurso de segurança. A solução não impede completamente o roubo de dados, mas fornece algum nível de impedimento e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar este recurso, recomendamos que você o combine com outras soluções de segurança, conforme aplicável.

> A marca d'água da sessão é um texto e é aplicada à sessão que é entregue ao usuário. A marca d'água da sessão contém informações para rastrear o roubo de dados. Os dados mais importantes são a identidade do usuário de logon da sessão atual na qual a imagem da tela foi tirada. Para rastrear o vazamento de dados de forma mais eficaz, inclua outras informações, como o endereço IP do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as configurações da política de Marca d'água da sessão para configurar o posicionamento e a aparência da marca d'água na tela.

**Requisitos:**

Agentes de Entrega Virtual:

SO multissessão 7.17 SO de sessão única 7.17

**Limitações:**

- As marcas d'água de sessão não são suportadas em sessões onde Acesso a Aplicativos Locais, redirecionamento de mídia do Windows, MediaStream, redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5 são usados. Para usar a marca d'água de sessão, certifique-se de que esses recursos estejam desativados.
- A marca d'água de sessão não é suportada e não aparece se a sessão estiver sendo executada em modos acelerados por hardware em tela cheia (codificação H.264 ou H.265 em tela cheia).
- Se você definir estas políticas HDX™, as configurações de marca d'água não terão efeito e uma marca d'água não será exibida na exibição da sessão.

**Usar codificação de hardware para codec de vídeo** para **Habilitado Usar codec de vídeo para compactação** para **Para a tela inteira**

- Se você definir essas políticas HDX, o comportamento é indeterminado e a marca d'água pode não ser exibida.

  **Usar codificação de hardware para codec de vídeo** para **Ativado Usar codec de vídeo para compactação** para **Usar codec de vídeo quando preferencial**

  Para garantir que a marca d'água seja exibida, defina **Usar codificação de hardware para codec de vídeo** como **Desativado**, ou defina **Usar codec de vídeo para compactação** como **Para regiões em mudança ativa** ou **Não usar codec de vídeo**.
- A marca d'água de sessão suporta apenas o modo gráfico Thinwire.
- Se você usa o Session Recording, a sessão gravada não inclui a marca d'água.
- Se você usa a assistência remota do Windows, a marca d'água não é exibida.
- Se um usuário pressionar a tecla **Print Screen** para capturar a tela, a tela capturada no lado do VDA não incluirá as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

# Compartilhamento de tela

O compartilhamento de tela permite que um usuário compartilhe uma sessão do Citrix Virtual Desktop com outros, incluindo conteúdo da tela, teclado e controles do mouse.

## Requisitos do sistema

- Windows: VDA de SO de sessão única ou multissessão
- Linux: Consulte a documentação do Linux VDA para obter mais informações sobre o compartilhamento de sessões Linux.
- Somente sessões de desktop podem ser compartilhadas.
- Deve haver conectividade de rede entre o VDA que hospeda a sessão e as máquinas que se conectam às sessões compartilhadas. Os requisitos de porta de rede são baseados nas portas ICA em uso (TCP/UDP 1494 ou 2598) e na configuração da política de compartilhamento de tela (TCP 52525 a 52625 por padrão).

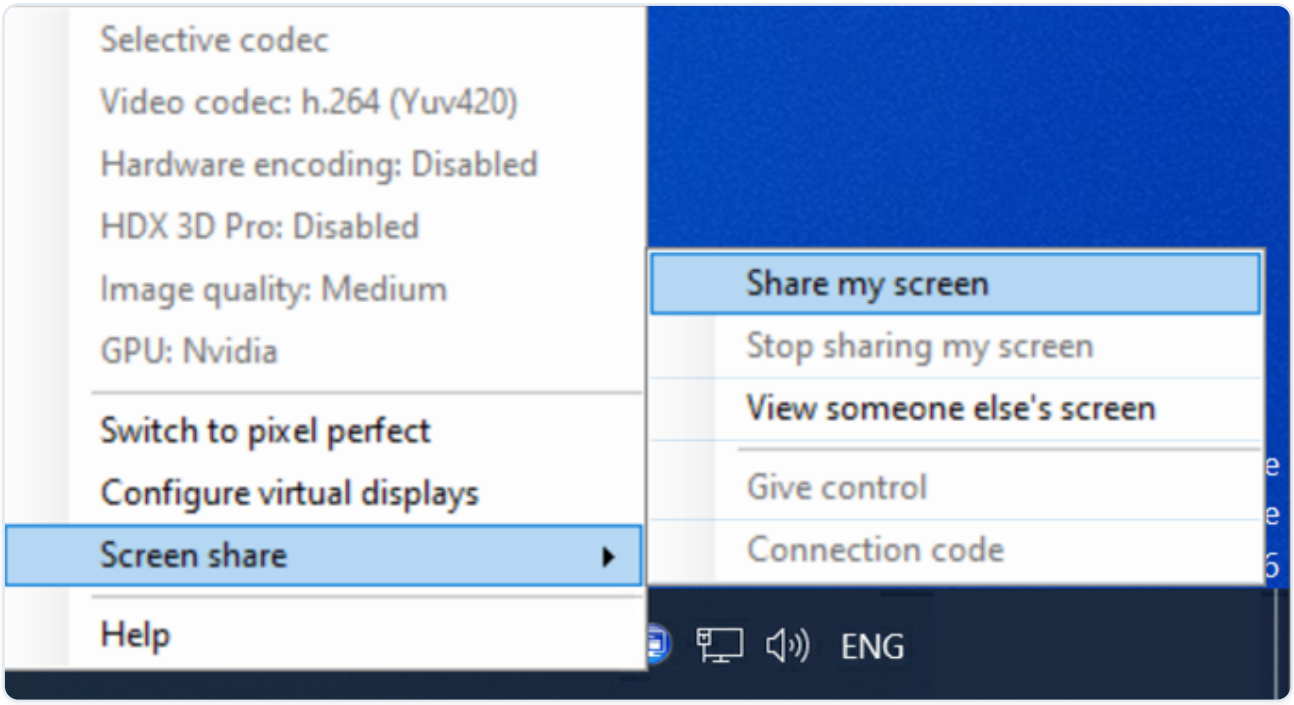
## Configuração

O compartilhamento de tela deve ser habilitado usando políticas Citrix. O compartilhamento de tela é desabilitado por padrão. Configure a política de compartilhamento de tela para habilitar ou desabilitar a função e atribuir o intervalo de portas de rede utilizável.

Habilite a política de indicador de status gráfico para exibir a interface do usuário que inclui controles para compartilhar e conectar-se a sessões.

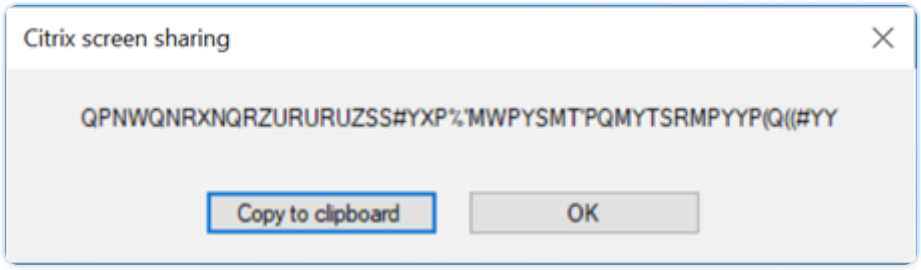
## Compartilhando uma sessão

Para compartilhar uma sessão, procure o ícone do indicador de status gráfico HDX™ na área de notificação do Windows. Clique com o botão direito nele para exibir o menu e selecione **Compartilhamento de tela > Compartilhar minha tela**.




Clique em **Copiar para a área de transferência** ou selecione e copie manualmente a string inteira mostrada na caixa de diálogo. A string pode então ser colada no aplicativo de sua escolha, como um cliente de e-mail ou de mensagens instantâneas, para ser distribuída a outros usuários.

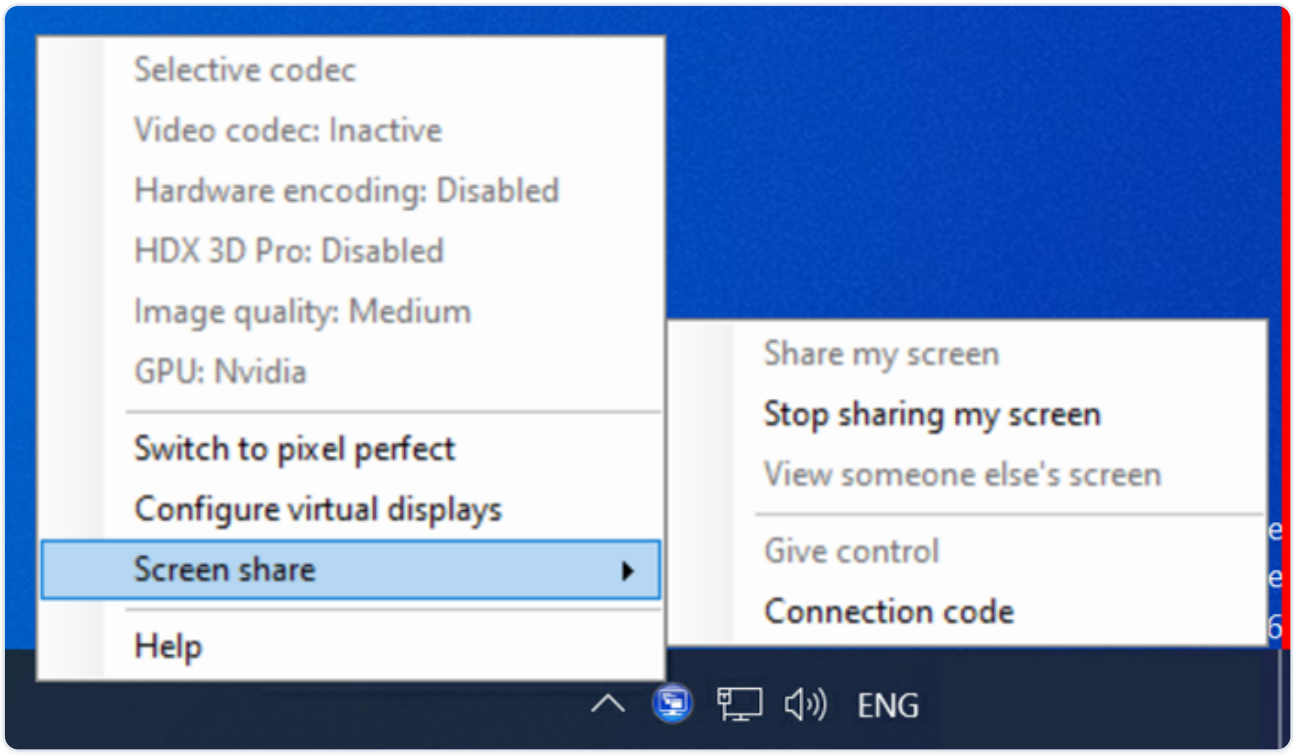
Clique em **OK** ou no **x** para fechar a caixa de diálogo. O código de conexão pode ser recuperado na opção de menu **Compartilhamento de tela > Código de conexão** a qualquer momento enquanto a sessão estiver sendo compartilhada.




Uma borda vermelha aparece ao redor da tela como um indicador de que a sessão está sendo compartilhada e está visível para outras pessoas.

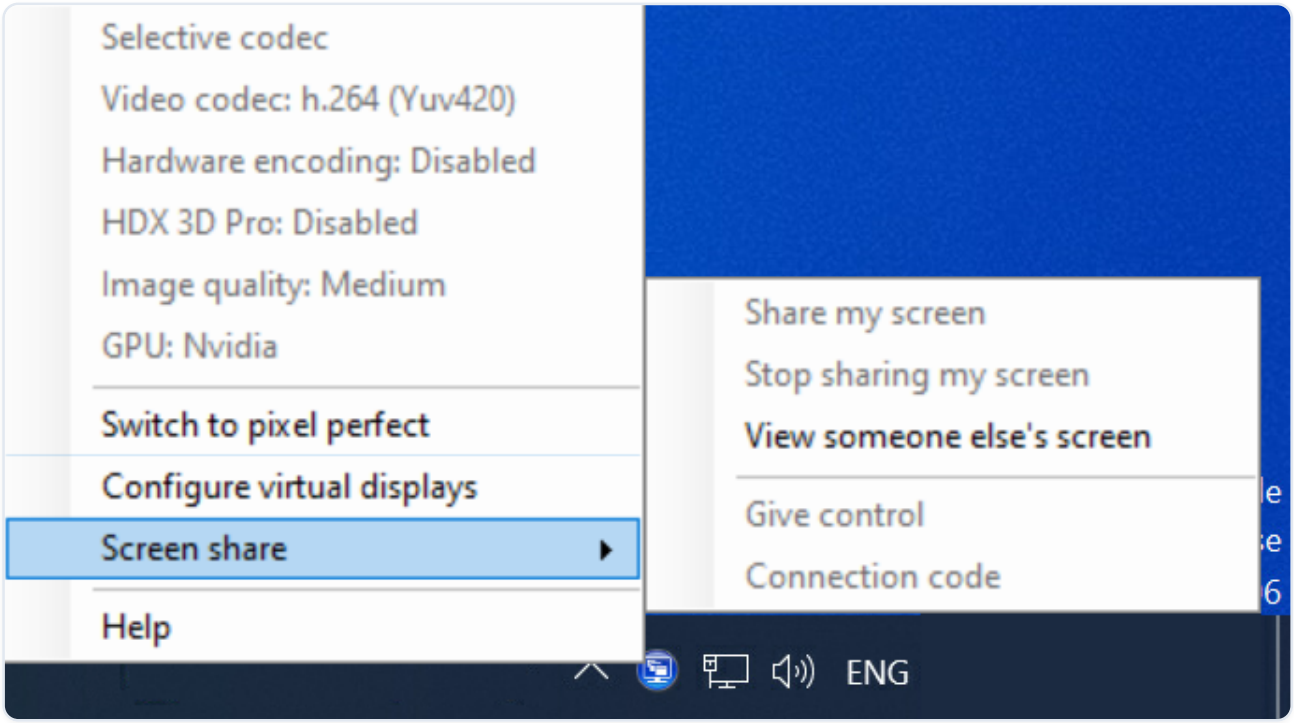
Os controles de teclado e mouse também podem ser compartilhados com outros usuários usando a opção de menu **Compartilhamento de tela > Conceder controle**.

Use a opção de menu **Compartilhamento de tela > Parar de compartilhar minha tela** para parar de compartilhar a sessão e desconectar todos os usuários.

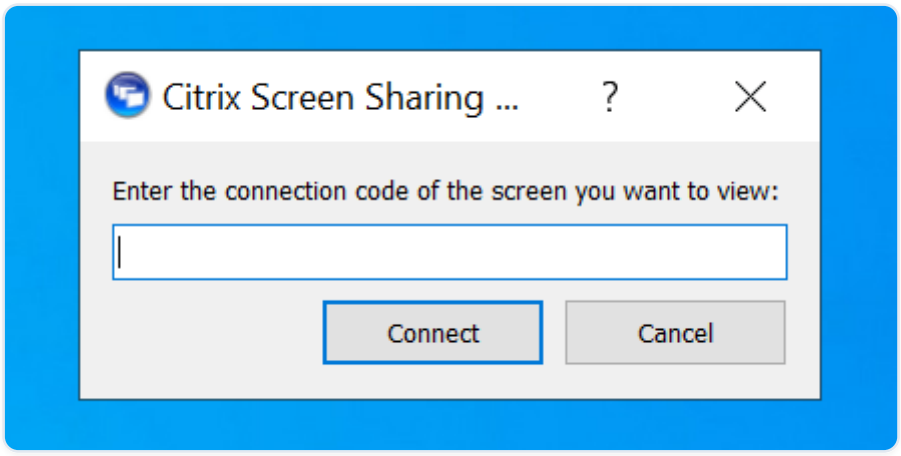



## Conectando-se a uma sessão compartilhada

Para se conectar às sessões de outra pessoa, procure o ícone do indicador de status gráfico HDX na área de notificação do Windows. Clique com o botão direito nele para exibir o menu e selecione **Compartilhamento de tela > Visualizar a tela de outra pessoa**.

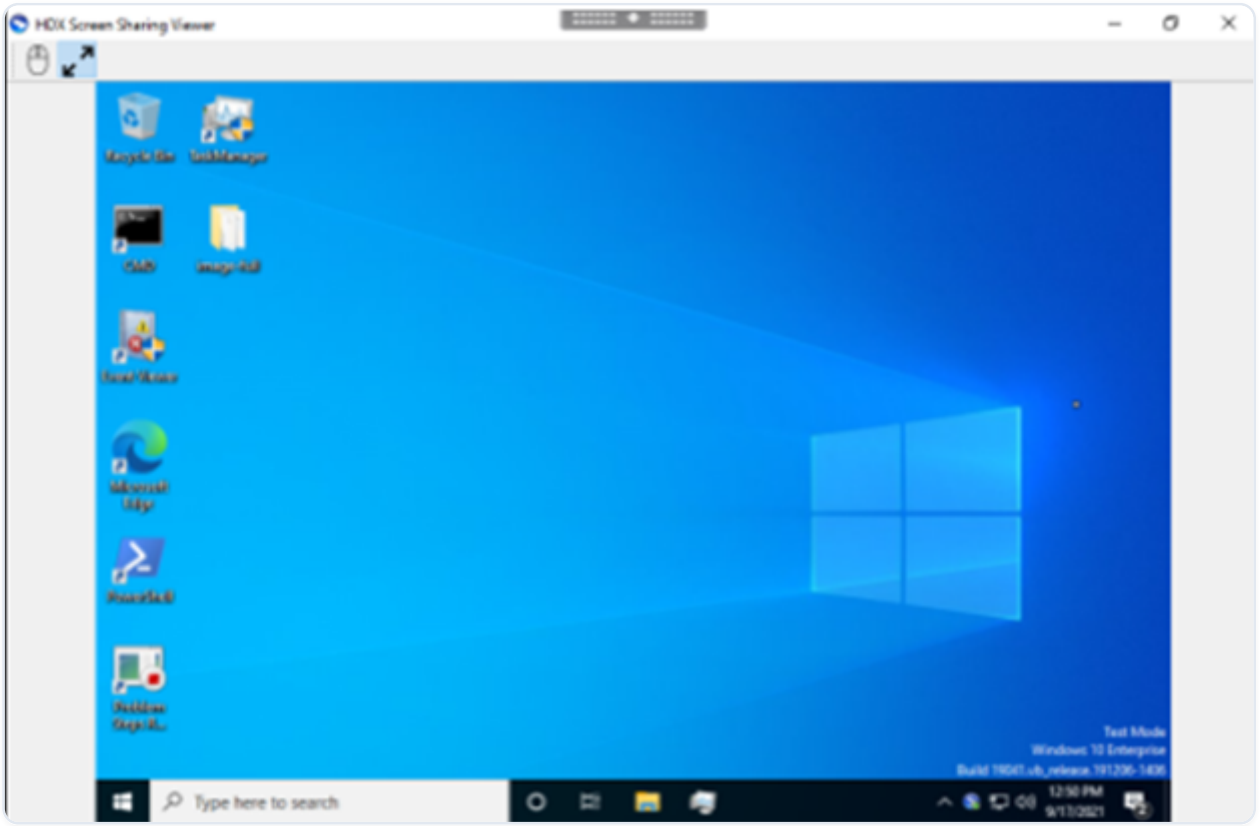



Insira ou cole a string de conexão fornecida pelo usuário que está compartilhando a sessão na caixa de texto. Clique em **Conectar** para estabelecer a conexão.




Você pode solicitar controles de teclado e mouse clicando no ícone do mouse no canto superior esquerdo da janela **HDX Screen Sharing Viewer**.

Feche a janela **HDX Screen Sharing Viewer** para desconectar-se da sessão compartilhada a qualquer momento.



## Outras considerações

- O aplicativo visualizador de compartilhamento de tela está incluído no VDA em *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* e pode ser implantado como um aplicativo publicado usando um Virtual Apps Server. Este modelo de implantação alternativo permite a colaboração com usuários que não têm acesso a um desktop virtual.

- O número de usuários permitidos para se conectar a uma sessão compartilhada pode ser limitado usando o intervalo de portas de rede na política de compartilhamento de tela. Uma porta é necessária por usuário. O intervalo padrão permite no máximo 100 usuários.
- Todos os monitores conectados à sessão são compartilhados. Não é possível selecionar monitores individuais.
- O codec de vídeo H.265 não é suportado.

# Layout de exibição virtual

A interface de usuário de configuração de exibição virtual permite definir um layout de exibição virtual por monitor de sessão no VDA, dentro de uma sessão ativa. Este recurso permite dividir cada monitor de sessão independentemente em vários monitores virtuais. Você pode dividir em um total de 8 monitores virtuais na área de trabalho remota. Além disso, você pode atualizar o monitor principal da sessão e as configurações de DPI para as exibições.

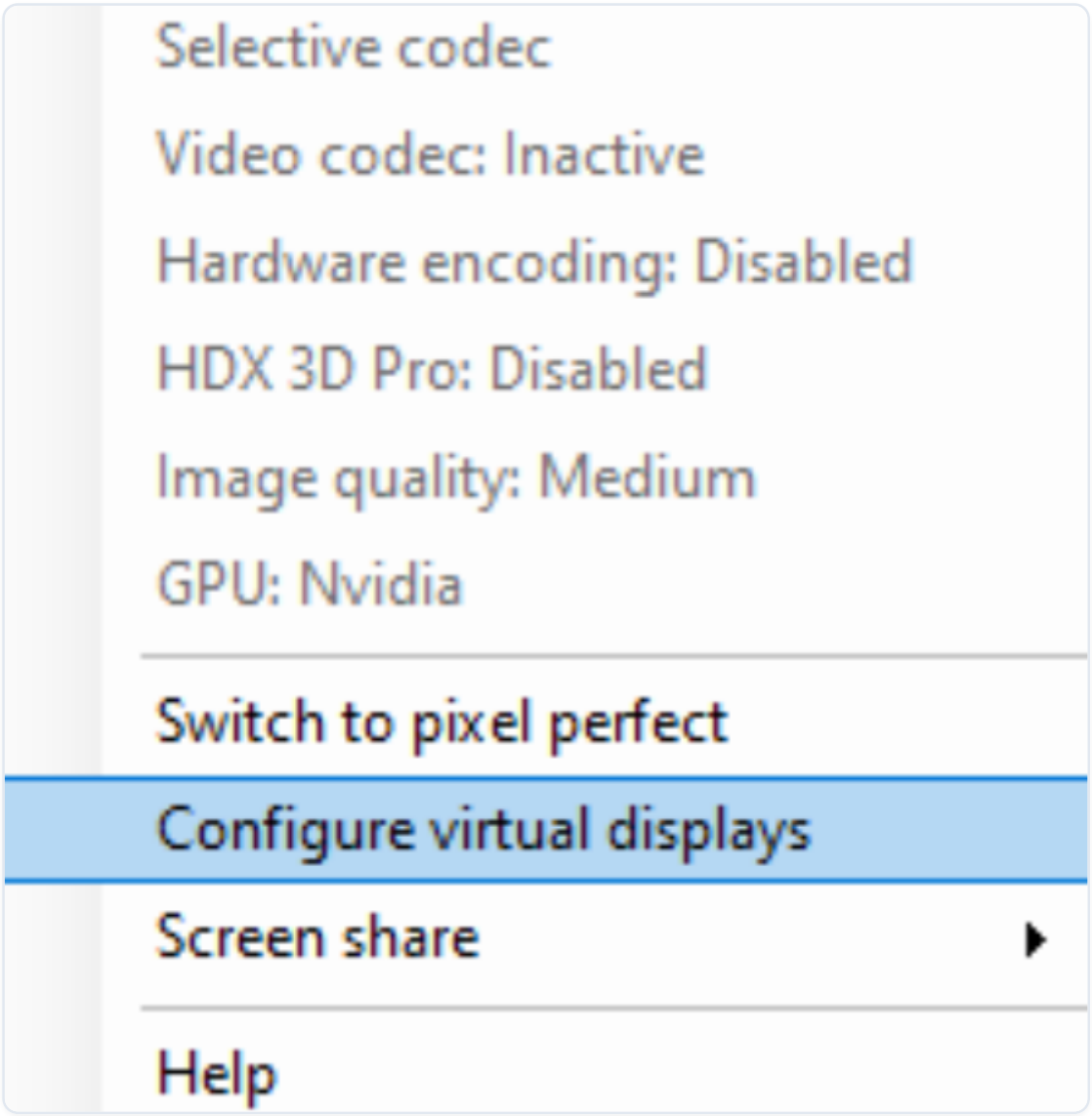
A configuração de exibição virtual é armazenada por usuário por dispositivo cliente. A configuração se aplica a todas as conexões subsequentes de um determinado cliente para um usuário específico. Ela é persistida durante o redimensionamento da sessão, desconexão ou reconexão da sessão, e logoff ou logon da sessão. A redefinição do layout de exibição virtual configurado ocorre no redimensionamento da sessão e na alteração do número de monitores de sessão.

## Requisitos do sistema

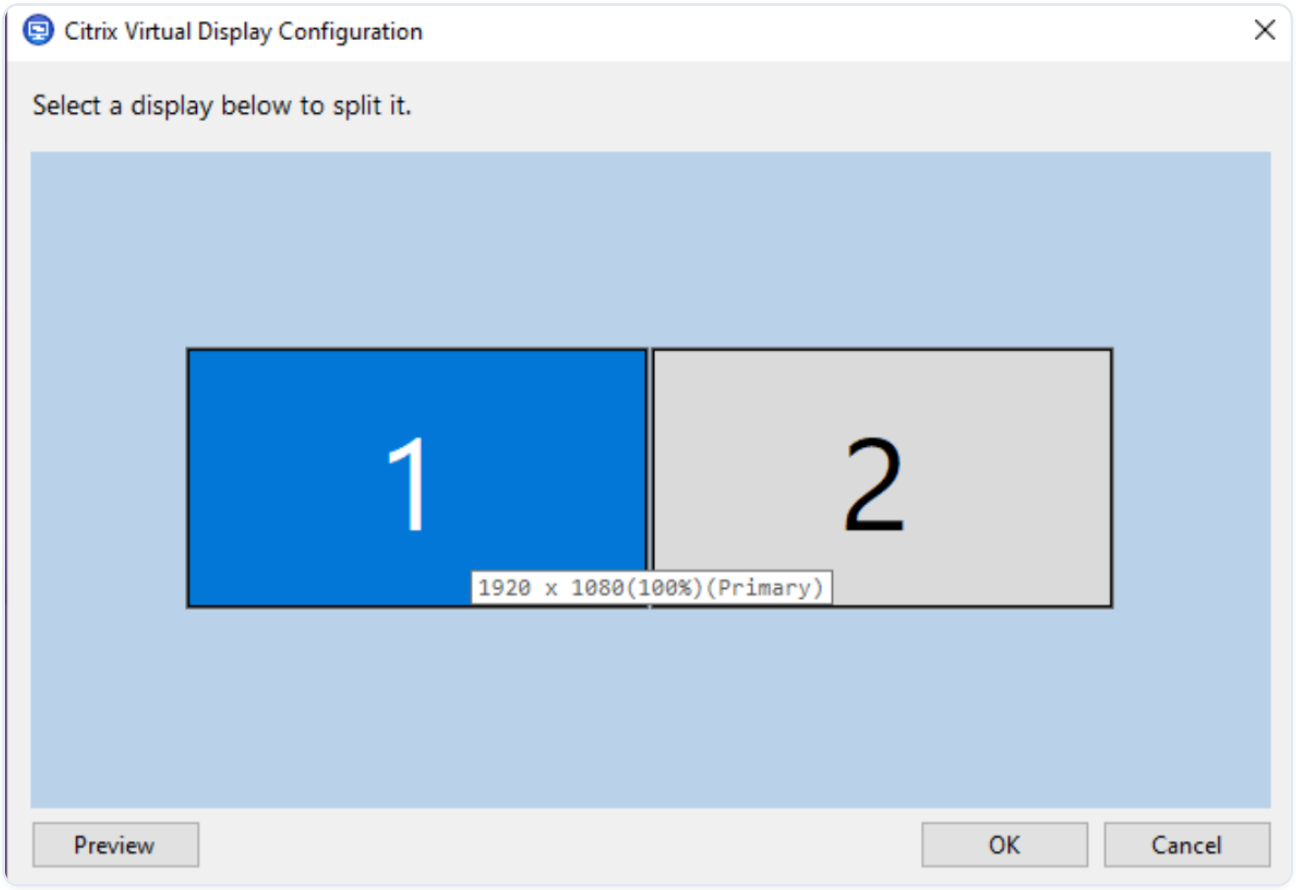
- Windows: VDA de SO de sessão única ou multi-sessão
- A política Indicador de status gráfico deve estar habilitada
- Somente sessões de desktop podem ser configuradas.

## Configuração

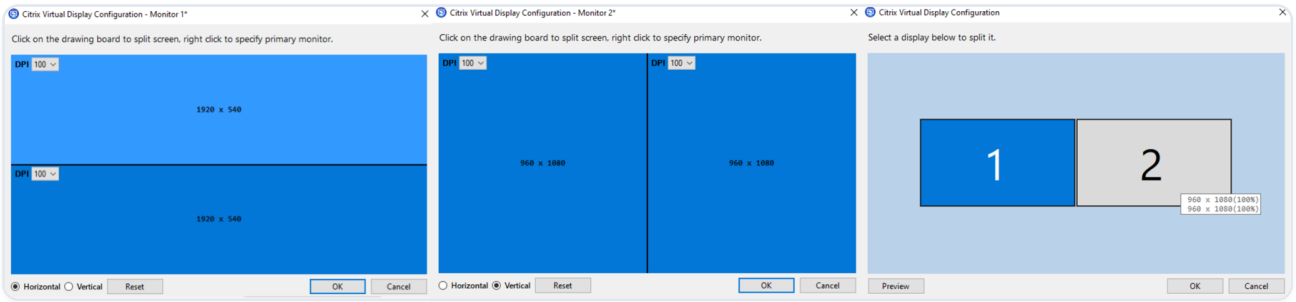
Para configurar o layout de exibição virtual, clique com o botão direito do mouse no ícone do indicador de status gráfico e selecione a opção Configurar exibições virtuais. A interface de usuário de configuração de exibição virtual é iniciada.



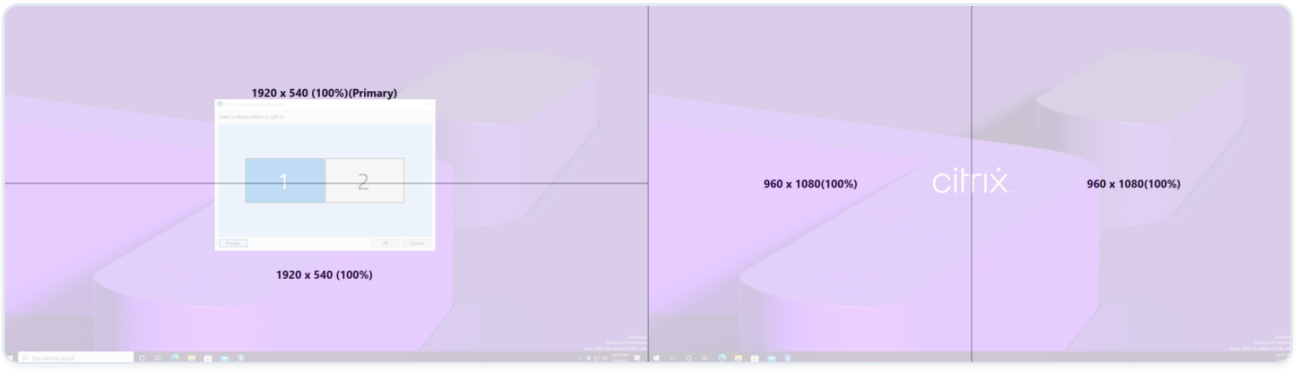

A interface de usuário mostra o layout de exibição da sessão atual, com o azul indicando o monitor principal da sessão. Você pode ver a dica de ferramenta de Configurações de exibição ao passar o mouse sobre uma exibição. A dica de ferramenta fornece informações sobre o layout de exibição virtual atual definido em um determinado monitor de sessão.



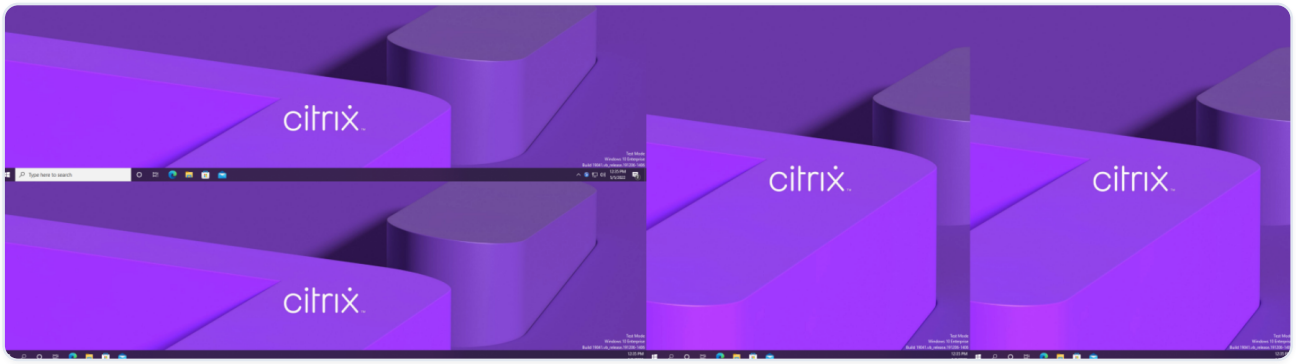

Selecione uma exibição para fazer a transição para uma interface de usuário interativa, que permite configurar exibições virtuais para o monitor de sessão selecionado. Você pode desenhar linhas horizontais ou verticais para separar a tela em monitores virtuais. A tela é dividida de acordo com porcentagens especificadas das resoluções do monitor de sessão. Clique com o botão direito do mouse em uma exibição virtual para marcá-la como monitor principal e use a lista suspensa de DPI para definir um fator de escala preferencial para a exibição virtual. Depois de definir um layout de exibição virtual, clique em **OK** para salvar temporariamente o layout ou em **Cancelar** para descartar quaisquer alterações. Você pode usar **Redefinir** para desfazer a configuração e restaurar o layout original para o monitor de sessão.



Para visualizar o layout de exibição virtual configurado atualmente, clique no botão **Visualizar**. Uma janela aparece para destacar a posição e a resolução esperadas das exibições virtuais na sessão.




Clique em **OK** para aplicar e salvar imediatamente o layout de exibição virtual. Clique em **Cancelar** para fechar a interface de usuário e descartar todas as alterações.

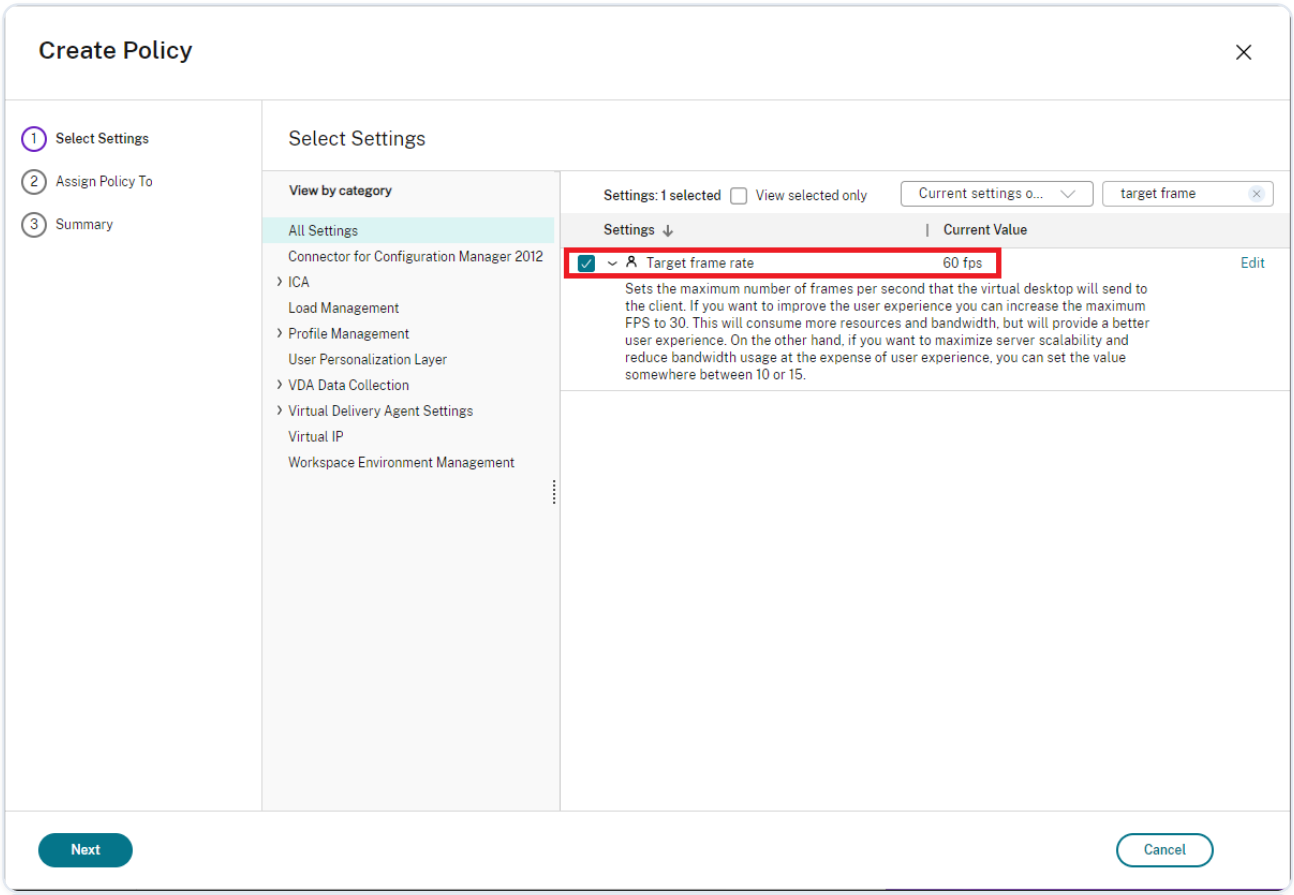


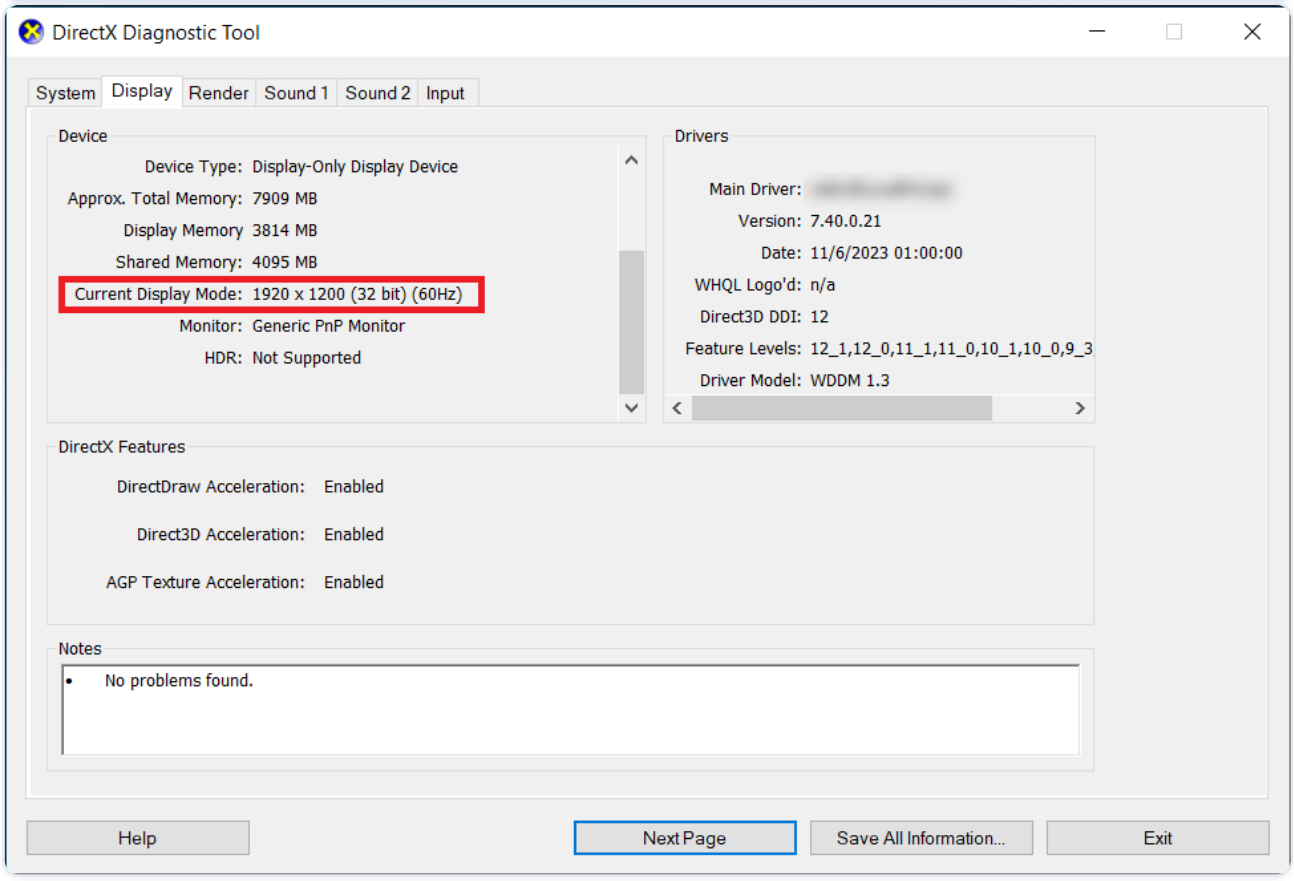
### Outras considerações

- A resolução mínima de tela virtual necessária é 640 x 480.
- O DPI da tela virtual definido através da interface do usuário depende do suporte de dimensionamento do SO para a resolução de tela fornecida.
- Não use este recurso simultaneamente com o recurso de tela virtual existente no aplicativo Citrix Workspace™.
- A funcionalidade de visualização não é suportada no Server 2016.

## Taxa de Atualização Adaptável

Com as novas melhorias de escalabilidade, o HDX™ ajusta a taxa de atualização dos monitores virtuais para corresponder à política de FPS de destino definida. A Taxa de Atualização Adaptável (ARR) está disponível para VDAs de sessão única e multissessão, e funciona para cenários acelerados por GPU e não-GPU.


Create Policy
1 Select Settings
2 Assign Policy To
3 Summary
Select Settings
View by category
All Settings
Connector for Configuration Manager 2012
ICA
Load Management
Profile Management
User Personalization Layer
VDA Data Collection
Virtual Delivery Agent Settings
Virtual IP
Workspace Environment Management
Settings: 1 selected
View selected only
Current settings o...
target frame
Settings
Current Value
Target frame rate
60 fps
Edit
Sets the maximum number of frames per second that the virtual desktop will send to the client. If you want to improve the user experience you can increase the maximum FPS to 30. This will consume more resources and bandwidth, but will provide a better user experience. On the other hand, if you want to maximize server scalability and reduce bandwidth usage at the expense of user experience, you can set the value somewhere between 10 or 15.
Next
Cancel


DirectX Diagnostic Tool
System
Display
Render
Sound 1
Sound 2
Input
Device
Device Type: Display-Only Display Device
Approx. Total Memory: 7909 MB
Display Memory 3814 MB
Shared Memory: 4095 MB
Current Display Mode: 1920 x 1200 (32 bit) (60Hz)
Monitor: Generic PnP Monitor
HDR: Not Supported
Drivers
Main Driver:
Version: 7.40.0.21
Date: 11/6/2023 01:00:00
WHQL Logo'd: n/a
Direct3D DDI: 12
Feature Levels: 12_1,12_0,11_1,11_0,10_1,10_0,9_3
Driver Model: WDDM 1.3
DirectX Features
DirectDraw Acceleration: Enabled
Direct3D Acceleration: Enabled
AGP Texture Acceleration: Enabled
Notes
No problems found.
Help
Next Page
Save All Information...
Exit

## Observação

> A Taxa de Atualização Adaptável está disponível apenas quando o Citrix Indirect Display ou IDD é usado (conforme o padrão do Citrix Virtual Apps and Desktops™) e não está disponível ao usar Adaptadores de Exibição fornecidos pelo Fornecedor.

## Modo tolerante a perdas para gráficos

O modo tolerante a perdas para gráficos foi completamente reformulado para garantir que a sessão permaneça interativa quando a perda de pacotes é detectada. Quando as condições da rede se degradam além dos limites predefinidos de largura de banda, latência e perda de pacotes, o codificador gráfico Citrix® muda automaticamente para um modo mais agressivo de entrega de pacotes para superar o efeito da perda de pacotes. Como resultado, o uso da largura de banda aumenta em uma quantidade proporcional à quantidade de perda de pacotes. Se as condições melhorarem posteriormente, o codificador gráfico Citrix muda de volta sem problemas. Os limites podem ser configurados via política, sendo os padrões 300 ms de latência e 5% de perda de pacotes.

O aplicativo Citrix Workspace™ para Windows 2311 é atualmente suportado. O suporte para outras plataformas será adicionado em versões posteriores do aplicativo Citrix Workspace. Assim como nas versões anteriores deste recurso, o HDX™ Adaptive Transport (EDT) deve estar habilitado para que este recurso funcione. Além disso, se a conexão for feita através do Citrix Gateway Service, o modo tolerante a perdas para gráficos também deve ser habilitado no Gateway.

# Multimídia

A pilha de tecnologia HDX™ suporta a entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia com renderização no lado do servidor
- Redirecionamento de multimídia com renderização no lado do cliente

Essa estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, enquanto maximiza a escalabilidade do servidor para reduzir o custo por usuário.

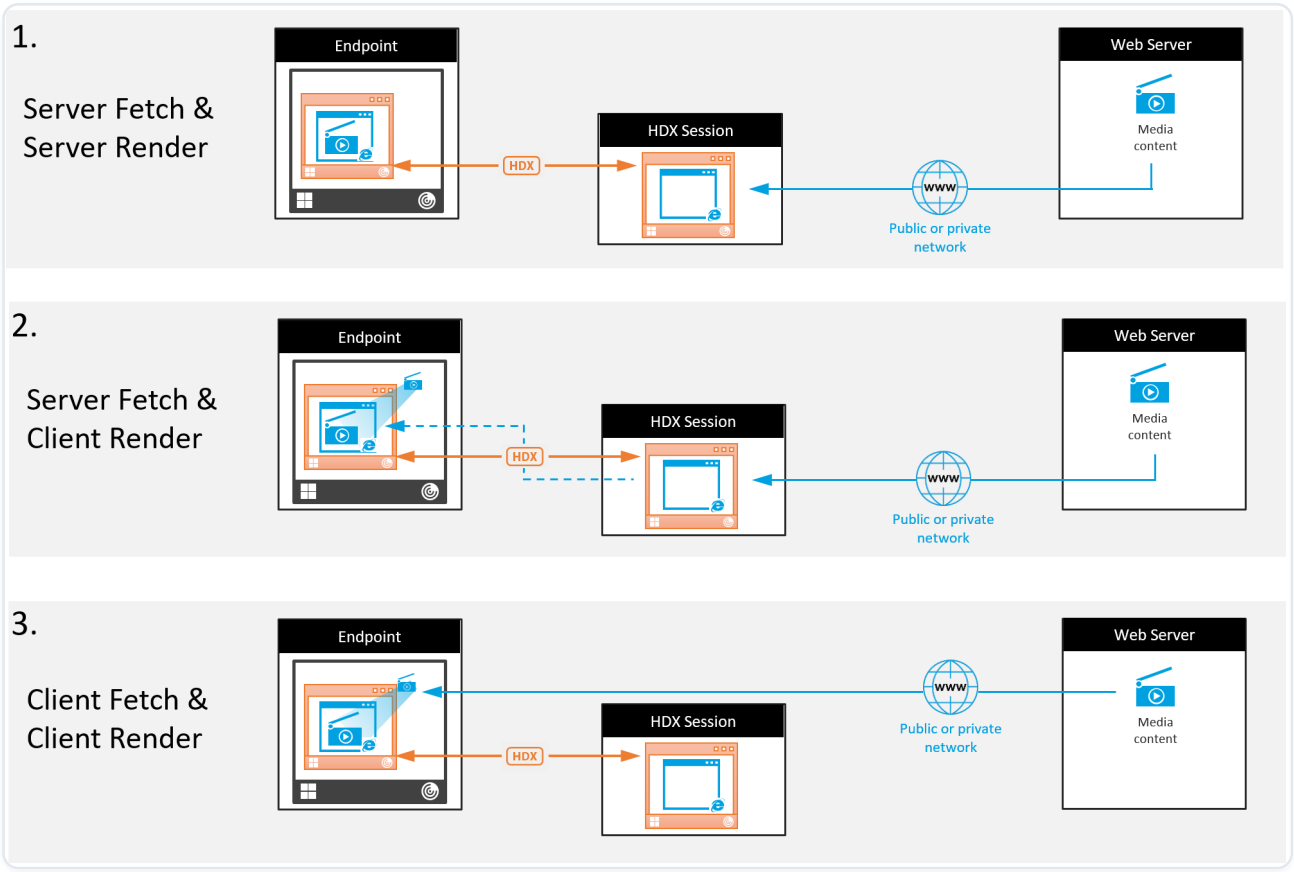
Com a entrega de multimídia renderizada no servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor Citrix Virtual Apps and Desktops pelo aplicativo. O conteúdo é então compactado e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo é intensivo em computação, a entrega de multimídia renderizada no servidor se beneficia muito da aceleração de hardware integrada. Por exemplo, o suporte para DirectX Video Acceleration (DXVA) descarrega a CPU realizando a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

Como a maioria dos servidores não oferece aceleração de hardware para compactação de vídeo, a escalabilidade do servidor é negativamente impactada se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter alta escalabilidade do servidor, redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

- O redirecionamento do Windows Media descarrega o servidor para uma ampla variedade de formatos de mídia tipicamente associados ao Windows Media Player.
- O vídeo HTML5 tornou-se popular, e a Citrix® introduziu uma tecnologia de redirecionamento para este tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento de contato Redirecionamento Host-para-cliente e Acesso a Aplicativos Locais ao conteúdo multimídia.

Juntando essas tecnologias, se você não configurar o redirecionamento, o HDX fará a Renderização no Lado do Servidor. Se você configurar o redirecionamento, o HDX usará a Busca no Servidor e Renderização no Cliente ou a Busca no Cliente e Renderização no Cliente. Se esses métodos falharem, o HDX retornará à Renderização no Lado do Servidor conforme necessário e estará sujeito à Política de Prevenção de Fallback.

# Cenários de exemplo




**Cenário 1. (Busca no Servidor e Renderização no Servidor):**

1. O servidor busca o arquivo de mídia de sua origem, decodifica e, em seguida, apresenta o conteúdo a um dispositivo de áudio ou dispositivo de exibição.
2. O servidor extrai a imagem ou som apresentados do dispositivo de exibição ou dispositivo de áudio, respectivamente.
3. O servidor, opcionalmente, o compacta e, em seguida, o transmite para o cliente.

Essa abordagem acarreta um alto custo de CPU, alto custo de largura de banda (se a imagem/som extraído não for compactado de forma eficiente) e tem baixa escalabilidade do servidor.

Os canais virtuais Thinwire e Áudio manipular essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para os clientes. Usando essa abordagem, a

decodificação acontece no servidor e funciona para uma variedade maior de dispositivos e formatos.

**Cenário 2. (Busca pelo Servidor e Renderização pelo Cliente):**

Essa abordagem depende da capacidade de interceptar o conteúdo de mídia antes que ele seja decodificado e apresentado ao dispositivo de áudio ou exibição. O conteúdo de áudio/vídeo compactado é, em vez disso, enviado ao cliente, onde é então decodificado e apresentado localmente. A vantagem dessa abordagem é que as tarefas são descarregadas para os dispositivos clientes, economizando ciclos de CPU no servidor.

No entanto, também introduz alguns requisitos adicionais de hardware e software para o cliente. O cliente deve ser capaz de decodificar cada formato que possa receber.

**Cenário 3. (Busca pelo Cliente e Renderização pelo Cliente):**

Essa abordagem depende da capacidade de interceptar a URL do conteúdo de mídia antes que ela seja buscada na origem. A URL é enviada ao cliente, onde o conteúdo de mídia é buscado, decodificado e apresentado localmente. Essa abordagem é conceitualmente simples. Sua vantagem é que ela economiza ciclos de CPU no servidor e largura de banda, pois o servidor envia apenas comandos de controle. No entanto, o conteúdo de mídia nem sempre está acessível aos clientes.

**Estrutura e plataforma:**

Sistemas operacionais de sessão única (Windows, Mac OS X e Linux) fornecem estruturas multimídia que permitem o desenvolvimento mais rápido de aplicativos multimídia. Esta tabela lista algumas das estruturas multimídia mais populares. Cada estrutura divide o processamento de mídia em várias etapas e usa uma arquitetura baseada em pipeline.

| ESTRUTURA | PLATAFORMA |
|---|---|
| DirectShow | Windows (98 e posterior) |
| Media Foundation | Windows (Vista e posterior) |
| Gstreamer | Linux |
| Quicktime | Mac OS X |

# Suporte a salto duplo com tecnologias de redirecionamento de mídia

| | |
|---|---|
| Redirecionamento de áudio | Não |
| Redirecionamento de conteúdo do navegador | Não |
| Redirecionamento de webcam HDX | Sim |
| Redirecionamento de vídeo HTML5 | Sim |
| Redirecionamento de Mídia do Windows | Sim |

# Recursos de áudio

Você pode configurar e adicionar as seguintes configurações de política do Citrix a uma política que otimiza os recursos de áudio HDX. Para detalhes de uso, além de relacionamentos e dependências com outras configurações de política, consulte Configurações de política de áudio, Configurações de política de largura de banda e Configurações de política de conexões multi-stream.

## Áudio adaptável

Com o áudio adaptável, você não precisa configurar manualmente as políticas de qualidade de áudio no VDA. O áudio adaptável otimiza as configurações para o seu ambiente e substitui formatos de compressão de áudio obsoletos para proporcionar uma excelente experiência ao usuário.

O áudio adaptável é ativado por padrão. Para desativar o áudio adaptável, consulte Configurações de política de áudio.

> **Importante:**
>
> A Citrix® recomenda a entrega de áudio usando o User Datagram Protocol (UDP) em vez de TCP quando aplicativos de áudio em tempo real são necessários. As seguintes opções de transporte de áudio estão disponíveis via UDP:
>
> - Áudio via UDP

- HDX™ Adaptive Transport (Enlightened Data Transport)

A criptografia de áudio UDP usando DTLS está disponível apenas entre o Citrix Gateway e o aplicativo Citrix Workspace™. Portanto, às vezes pode ser preferível usar o transporte TCP. O TCP oferece suporte à criptografia TLS de ponta a ponta do VDA para o aplicativo Citrix Workspace.

Para obter mais informações sobre áudio adaptável e áudio UDP, consulte Transporte em tempo real de áudio via UDP e intervalo de portas UDP de áudio.

## Modo tolerante a perdas para áudio

O modo tolerante a perdas suporta áudio. Este recurso aumenta a experiência do usuário para streaming em tempo real e melhora a qualidade do áudio via EDT quando os usuários se conectam através de redes com alta latência e perda de pacotes. Este recurso é desativado por padrão.

**Nota:**

Ambas as políticas **HDX Adaptive Transport (EDT)** e **modo tolerante a perdas para áudio** devem estar ativadas para que este recurso funcione.

### Requisitos do sistema

Certifique-se de que os seguintes produtos estejam nas versões mínimas que suportam o modo tolerante a perdas:

- Citrix Virtual Delivery Agent (VDA) 2308
- Citrix Workspace app para Windows 2309

Além disso, os seguintes recursos devem ser ativados:

- Política de HDX Adaptive Transport.
- (Opcional) Para conexões remotas, Citrix Gateway Service é necessário.

**Nota:**

> Se as condições acima não forem atendidas, o áudio é enviado pelo transporte confiável EDT.

### Informações adicionais

O modo tolerante a perdas é um protocolo de transporte tolerante a perdas que permite a perda de pacotes na transmissão sem reenviar conteúdo multimídia, resultando em uma experiência mais em tempo real para os usuários.

Enlightened Data Transport (EDT) é um protocolo de transporte proprietário da Citrix que oferece uma experiência de usuário superior em conexões de longa distância desafiadoras, mantendo a escalabilidade do servidor. O modo tolerante a perdas é um recurso do serviço Citrix Gateway que usa o modo tolerante a perdas como protocolo de transporte para manter uma conexão estável mesmo diante do congestionamento da rede. Isso garante uma experiência consistente e estável para trabalhadores remotos. Em condições normais, tanto o EDT quanto o modo tolerante a perdas fornecem resultados semelhantes. No entanto, em condições de rede com perda de pacotes, o modo tolerante a perdas oferece uma experiência de áudio melhor em comparação com o EDT. Isso o torna um recurso essencial para trabalhadores remotos que dependem de multimídia em tempo real para seu trabalho.

## Qualidade do áudio

Em geral, uma qualidade de som mais alta consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para os dispositivos do usuário. A compressão de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações de política do Citrix para configurar os níveis de compressão a serem aplicados aos arquivos de som.

Por padrão, a configuração da **política de qualidade de áudio** é definida como Alta - áudio de alta definição quando o transporte TCP é usado. A política é definida como Média - otimizada para fala quando o transporte UDP (recomendado) é usado. A configuração de **áudio de alta definição** fornece áudio estéreo de alta fidelidade, mas consome mais largura de banda do que outras configurações de qualidade. Não use esta qualidade de áudio para aplicativos de bate-papo por voz ou vídeo não otimizados (como softphones). O motivo é que isso pode introduzir latência no caminho do áudio, o que não é adequado para comunicações em tempo real. Recomendamos a configuração de política otimizada para fala para áudio em tempo real, independentemente do protocolo de transporte selecionado.

Quando a largura de banda é limitada, por exemplo, conexões via satélite ou discadas, reduzir a qualidade do áudio para **Baixa** consome a menor largura de banda possível. Nesta situação, crie políticas separadas para usuários em conexões de baixa largura de banda para que os usuários em conexões de alta largura de banda não sejam afetados negativamente.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Diretrizes de largura de banda para reprodução e gravação de áudio:

- Áudio adaptável (padrão)
  - Taxa de bits: adaptável variável
  - Número de canais: 2 (Estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 48000 Hz
  - Profundidade de bits: 16 bits
- Alta qualidade
  - Taxa de bits: ~100 kbps (mín. 75, máx. 175 kbps) para reprodução / ~70 kbps para captura de microfone
  - Número de Canais: 2 (Estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 44100 Hz
  - Profundidade de bits: 16 bits
- Qualidade média (recomendado para VoIP)
  - Taxa de bits: ~16 kbps (mín. 20, máx. 40 kbps) para reprodução, ~16 kbps para captura de microfone
  - Número de Canais: 1 (Mono) para reprodução e captura
  - Frequência: 16000 Hz (banda larga)
  - Profundidade de bits: 16 bits
- Qualidade baixa
  - Taxa de bits: ~ 11 kbps (mín. 10; máx. 25 kbps) para reprodução, ~11 kbps para captura de microfone
  - Número de Canais: 1 (Mono) para reprodução e captura
  - Frequência: 8000 Hz (banda estreita)

- Profundidade de bits: 16 bits

## Redirecionamento de áudio do cliente

Para permitir que os usuários recebam áudio de um aplicativo em um servidor através de alto-falantes ou outros dispositivos de som no dispositivo do usuário, deixe a configuração de **Redirecionamento de áudio do cliente** como **Permitido**. Esta é a configuração padrão.

O mapeamento de áudio do cliente sobrecarrega os servidores e a rede. No entanto, proibir o redirecionamento de áudio do cliente desabilita toda a funcionalidade de áudio HDX.

Para obter detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

## Redirecionamento de microfone do cliente

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Redirecionamento de microfone do cliente** em seu padrão (Permitido).

Por segurança, os dispositivos do usuário alertam seus usuários quando servidores em que não confiam tentam acessar microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar este alerta no aplicativo Citrix Workspace.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

## Plug N Play de áudio

A configuração de política Plug N Play de áudio permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração está **Habilitada** por padrão. O Plug N Play de áudio permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até depois do início da sessão do usuário.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Para detalhes das configurações, consulte Configurações de política de áudio.

## Limite de largura de banda de redirecionamento de áudio e porcentagem de limite de largura de banda de redirecionamento de áudio

A configuração de política Limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para reprodução e gravação de áudio em uma sessão.

A configuração Porcentagem de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima para redirecionamento de áudio como uma porcentagem da largura de banda total disponível.

Por padrão, zero (sem máximo) é especificado para ambas as configurações. Se ambas as configurações forem configuradas, a que tiver o menor limite de largura de banda será usada.

Para detalhes das configurações, consulte Configurações de política de largura de banda. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

## Áudio sobre transporte em tempo real UDP e intervalo de porta UDP de áudio

Por padrão, o Áudio sobre Transporte em Tempo Real do Protocolo de Datagrama de Usuário (UDP) é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam Áudio sobre Transporte em Tempo Real UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar UDP/RTP para áudio para garantir a melhor experiência possível ao usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio UDP é preferível ao EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que nenhuma latência seja adicionada em conexões com alta perda de pacotes.

> **Importante:**

> Quando o Citrix Gateway não está no caminho, os dados de áudio transmitidos com UDP não são criptografados. Se o Citrix Gateway estiver configurado para acessar recursos do Citrix Virtual Apps and Desktops™, o tráfego de áudio entre o dispositivo de endpoint e o Citrix Gateway é protegido usando o protocolo DTLS.

> O intervalo de porta UDP de áudio especifica o intervalo de números de porta que o VDA do Windows usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é de 16500 a 16509.

> **Nota:**
>
> Se o Áudio sobre Transporte UDP em Tempo Real não for necessário para áudio adaptável, a Citrix recomenda configurar a política para Desativado. Isso ajuda a evitar que os clientes do aplicativo Citrix Workspace solicitem conexões UDP abertas ou acionem o aparecimento de janelas de diálogo de configuração de firewall do cliente do aplicativo Citrix Workspace indesejadas.

> Para obter detalhes de configuração sobre Áudio sobre UDP Real-time Transport, consulte Configurações de política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações de política de conexões multi-stream. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre UDP requer o VDA do Windows. Para políticas suportadas no VDA do Linux, consulte Lista de suporte de políticas.

## Políticas de configuração de áudio para dispositivos de usuário

1. Carregue os modelos de política de grupo seguindo Configurando o modelo administrativo do Objeto de Política de Grupo.
2. No Editor de Política de Grupo, expanda **Modelos Administrativos > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Para **Configurações de áudio do cliente**, selecione **Não Configurado**, **Habilitado** ou **Desabilitado**.
   - **Não Configurado**. Por padrão, o Redirecionamento de Áudio é habilitado usando áudio de alta qualidade ou as configurações de áudio personalizadas configuradas anteriormente.
   - **Habilitado**. Habilita o redirecionamento de áudio usando as opções selecionadas.
   - **Desabilitado**. Desabilita o redirecionamento de áudio.
4. Se você selecionar **Habilitado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Habilitar Transporte em Tempo Real** e então defina o intervalo de portas de entrada a serem abertas no firewall local do Windows.

6. Para usar Áudio UDP com Citrix Gateway, selecione **Permitir Transporte em Tempo Real Através do gateway**. Configure o Citrix Gateway com DTLS. Para mais informações, consulte este artigo.

Como Administrador, se você não tiver controle sobre os dispositivos de endpoint para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o Áudio UDP. Por exemplo, para dispositivos pessoais ou computadores domésticos.

1. Na máquina StoreFront, abra C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica com um editor como o notepad.
2. Faça as seguintes entradas na seção .

   ; Este texto habilita o Transporte em Tempo Real

   EnableRtpAudio=true

   ; Este texto permite o Transporte em Tempo Real Através do gateway

   EnableUDPThroughGateway=true

   ; Este texto define a qualidade do áudio como Média

   AudioBandwidthLimit=1

   ; Intervalo de portas UDP

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Se você habilitar o áudio do User Datagram Protocol (UDP) editando default.ica, o áudio UDP será habilitado para todos os usuários que estiverem usando essa loja.

## Evitar eco durante conferências multimídia

Usuários em conferências de áudio ou vídeo podem ouvir um eco. Ecos geralmente ocorrem quando alto-falantes e microfones estão muito próximos um do outro. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX oferece uma opção de cancelamento de eco (ativada por padrão) que minimiza qualquer eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Certifique-se de que os dispositivos não estejam muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração de registro para desativar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados por meio do registro.

## Softphones

Um softphone é um software que atua como uma interface de telefone. Você usa um softphone para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Ao usar um softphone, você pode discar números de telefone e realizar outras funções relacionadas ao telefone usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para a entrega de softphones.

- **Modo de controle**. O softphone hospedado controla um aparelho telefônico físico. Neste modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.
- **Suporte a softphone otimizado para HDX RealTime (recomendado)**. O mecanismo de mídia é executado no dispositivo do usuário, e o tráfego de Voz sobre Protocolo de Internet flui de ponto a ponto. Para exemplos, consulte:
  - Otimização HDX para Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone para VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings para VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin VDI do Zoom
  - Genesys PureEngage Cloud
  - Dispositivo de ditado Nuance Dragon PowerMic
- **Acesso a Aplicativos Locais**. Um recurso do Citrix Virtual Apps and Desktops que permite que um aplicativo, como um softphone, seja executado localmente no dispositivo de usuário Windows, mas apareça perfeitamente integrado ao seu desktop virtual/publicado. Este recurso descarrega todo o processamento de áudio para o dispositivo do usuário. Para mais informações, consulte Acesso a Aplicativos Locais e redirecionamento de URL.
- **Suporte genérico a softphone HDX RealTime.** Voz sobre Protocolo de Internet sobre ICA.

***Suporte genérico a softphone***

O suporte genérico a softphones permite hospedar um softphone não modificado no XenApp ou XenDesktop no data center. O tráfego de áudio passa pelo protocolo Citrix ICA (preferencialmente usando UDP/RTP) para o dispositivo do usuário executando o aplicativo Citrix Workspace.

O suporte genérico a softphone é um recurso do HDX RealTime. Essa abordagem para entrega de softphone é especialmente útil quando:

- Uma solução otimizada para entregar o softphone não está disponível e o usuário não está em um dispositivo Windows onde o Acesso a Aplicativos Locais possa ser usado.
- O mecanismo de mídia necessário para a entrega otimizada do softphone não está instalado no dispositivo do usuário ou não está disponível para a versão do sistema operacional em execução no dispositivo do usuário. Nesse cenário, o HDX RealTime Genérico fornece uma solução de fallback valiosa.

Existem duas considerações sobre a entrega de softphone usando Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é entregue ao desktop virtual/publicado.
- Como o áudio é entregue para e do headset, microfone e alto-falantes do usuário, ou conjunto de telefone USB.

Citrix Virtual Apps and Desktops incluem inúmeras tecnologias para suportar a entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida do áudio em tempo real e eficiência de largura de banda.
- Pilha de áudio de baixa latência.
- Buffer de jitter do lado do servidor para suavizar o áudio quando a latência da rede flutua.
- Marcação de pacotes (DSCP e WMM) para Qualidade de Serviço.
    - Marcação DSCP para pacotes RTP (Camada 3)
    - Marcação WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voz sobre Protocolo de Internet. O aplicativo Citrix Workspace para Windows oferece estes recursos:

- Buffer de jitter do lado do cliente - Garante áudio suave mesmo quando a latência da rede flutua.

- Cancelamento de eco - Permite maior variação na distância entre o microfone e os alto-falantes para trabalhadores que não usam fone de ouvido.
- Áudio plug-n-play - Dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.
- Roteamento de dispositivo de áudio - Os usuários podem direcionar o toque para os alto-falantes, mas o caminho de voz para o fone de ouvido.
- ICA multi-stream - Permite roteamento flexível baseado em Qualidade de Serviço pela rede.
- O ICA suporta quatro fluxos TCP e dois UDP. Um dos fluxos UDP suporta o áudio em tempo real sobre RTP.

Para um resumo dos recursos do aplicativo Citrix Workspace, consulte Matriz de Recursos do Citrix Receiver.

***Recomendações de configuração do sistema***

*Hardware e Software do Cliente*: Para uma qualidade de áudio ideal, recomendamos a versão mais recente do aplicativo Citrix Workspace e um fone de ouvido de boa qualidade que tenha cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac suportam Voz sobre Protocolo de Internet. Além disso, a Dell Wyse oferece suporte a Voz sobre Protocolo de Internet para ThinOS (WTOS).

*Considerações sobre a CPU*: Monitore o uso da CPU no VDA para determinar se é necessário atribuir duas CPUs virtuais a cada máquina virtual. Voz e vídeo em tempo real são intensivos em dados. A configuração de duas CPUs virtuais reduz a latência de troca de threads. Portanto, recomendamos que você configure duas vCPUs em um ambiente VDI do Citrix Virtual Desktops™.

Ter duas CPUs virtuais não significa necessariamente dobrar o número de CPUs físicas, pois as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de Confiabilidade da Sessão, também aumenta o consumo de CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo de CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor poderoso.

*Áudio UDP*: O áudio sobre UDP oferece excelente tolerância a congestionamento de rede e perda de pacotes. Recomendamos usá-lo em vez de TCP quando disponível.

*Configuração de LAN/WAN*: A configuração adequada da rede é fundamental para uma boa qualidade de áudio em tempo real. Normalmente, você deve configurar redes locais virtuais (VLANs) porque pacotes de broadcast excessivos podem introduzir jitter. Dispositivos habilitados para IPv6 podem gerar muitos pacotes de broadcast. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configure para suportar Qualidade de Serviço.

*Configurações para uso de conexões WAN*: Você pode usar bate-papo por voz em conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se estiver entregando softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler® SD-WAN entre o data center e o escritório remoto. Isso mantém uma alta Qualidade de Serviço. O NetScaler SD-WAN suporta ICA Multi-Stream, incluindo UDP. Além disso, para um único fluxo TCP, é possível distinguir as prioridades de vários canais virtuais ICA para garantir que os dados de áudio em tempo real de alta prioridade recebam tratamento preferencial.

Use o Director ou o HDX Monitor para validar sua configuração HDX.

*Conexões de usuário remoto*: O Citrix Gateway suporta DTLS para entregar tráfego UDP/RTP nativamente (sem encapsulamento em TCP). Abra os firewalls bidirecionalmente para tráfego UDP na Porta 443.

*Seleção de codec e consumo de largura de banda*: Entre o dispositivo do usuário e o VDA no data center, recomendamos usar a configuração de codec **Otimizado para Fala**, também conhecida como áudio de Qualidade Média. Entre a plataforma VDA e o IP-PBX, o softphone usa o codec configurado ou negociado. Por exemplo:

- O G711 oferece boa qualidade de voz, mas tem um requisito de largura de banda de 80 kilobits por segundo a 100 kilobits por segundo por chamada (dependendo dos overheads da Camada 2 da Rede).
- O G729 oferece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo a 40 kilobits por segundo por chamada (dependendo dos overheads da Camada 2 da Rede).

***Entrega de aplicativos de softphone para o desktop virtual***

Existem dois métodos pelos quais você pode entregar um softphone ao desktop virtual XenDesktop®:

- O aplicativo pode ser instalado na imagem do desktop virtual.

- O aplicativo pode ser transmitido por streaming para o desktop virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciamento porque a imagem do desktop virtual é mantida organizada. Após ser transmitido por streaming para o desktop virtual, o aplicativo é executado nesse ambiente como se tivesse sido instalado da maneira usual. Nem todos os aplicativos são compatíveis com o App-V.

### *Entrega de áudio para e do dispositivo do usuário*

O HDX RealTime genérico suporta dois métodos de entrega de áudio para e do dispositivo do usuário:

- **Canal Virtual de Áudio Citrix**. Geralmente recomendamos o Canal Virtual de Áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB Genérico**. Suporta dispositivos de áudio com botões ou um display (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou similar à LAN de volta para o servidor Citrix Virtual Apps and Desktops.

### *Canal virtual de áudio Citrix*

O Canal Virtual de Áudio Bidirecional Citrix (CTXCAM) permite que o áudio seja entregue de forma eficiente pela rede. O HDX RealTime Genérico pega o áudio do headset ou microfone do usuário e o compacta. Em seguida, ele o envia via ICA para o aplicativo de softphone no desktop virtual. Da mesma forma, a saída de áudio do softphone é compactada e enviada na outra direção para o headset ou alto-falantes do usuário. Essa compactação é independente da compactação usada pelo próprio softphone (como G.729 ou G.711). Ela é feita usando o codec Otimizado para Fala (Qualidade Média). Suas características são ideais para Voz sobre Protocolo de Internet. Ele apresenta tempo de codificação rápido e consome apenas aproximadamente 56 Kilobits por segundo de largura de banda da rede (28 Kbps em cada direção), no pico. Este codec deve ser explicitamente selecionado no console do Studio porque não é o codec de áudio padrão. O padrão é o codec de Áudio HD (Alta Qualidade). Este codec é excelente para trilhas sonoras estéreo de alta fidelidade, mas é mais lento para codificar em comparação com o codec Otimizado para Fala.

### *Redirecionamento USB Genérico*

A tecnologia de Redirecionamento USB Genérico da Citrix (canal virtual CTXGUSB) fornece um meio genérico de acesso remoto a dispositivos USB, incluindo dispositivos compostos (áudio mais HID) e dispositivos USB isócronos. Essa abordagem é limitada a usuários conectados à LAN. A razão é que o protocolo USB tende a ser sensível à latência da rede e requer uma largura de banda considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones. Este redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o Canal

Virtual de Áudio Citrix é preferido porque é otimizado para tráfego de áudio. A principal exceção é quando você está usando um dispositivo de áudio com botões. Por exemplo, um telefone USB conectado ao dispositivo do usuário que está conectado à LAN do data center. Neste caso, o Redirecionamento USB Genérico suporta botões no aparelho telefônico ou headset que controlam recursos enviando um sinal de volta para o softphone. Não há problema com botões que funcionam localmente no dispositivo.

## Ferramenta de linha de comando de diagnóstico de áudio

A ferramenta de linha de comando de diagnóstico de áudio no VDA pode ser usada para consultar dados de sessão relacionados a políticas de áudio, configuração e transporte de dados.

### Uso

Abra um prompt de comando e execute `CtxAudio.exe` da pasta `C:\Program Files\Citrix\HDX\bin`.

- Executar a ferramenta como administrador exibe todas as informações de áudio da(s) sessão(ões) ICA ativa(s).
- Executar a ferramenta como não administrador exibe as informações de áudio da sessão ICA do usuário atual.

### Saída

A ferramenta exibe várias configurações que podem ajudar a diagnosticar problemas relacionados ao áudio em uma sessão.

| SEÇÃO | DESCRIÇÃO |
|---|---|
| Informações da política | Políticas de áudio aplicadas à(s) sessão(ões) atual(is). |
| Informações de configurações | Configurações relacionadas ao áudio armazenadas no registro. |
| Informações de estado | Estado do áudio, versão, codecs e transporte aplicados à(s) sessão(ões) atual(is). |
| Informações dos dispositivos | Nomes dos dispositivos, suas funções e seus status usados na sessão. |

> **Nota:**
>
> A saída varia dependendo se você executa a ferramenta em um VDA de várias sessões (TS) ou em um VDA de sessão única (WSVDA).

### Limitação

Você instala um dispositivo de áudio em seu cliente, habilita o redirecionamento de áudio e inicia uma sessão RDS. Os arquivos de áudio podem não ser reproduzidos e uma mensagem de erro aparece.

Como solução alternativa, adicione a chave do registro na máquina RDS e, em seguida, reinicie a máquina. Para obter informações, consulte Limitação de áudio na lista de recursos gerenciados por meio do registro.

## Redirecionamento de conteúdo do navegador

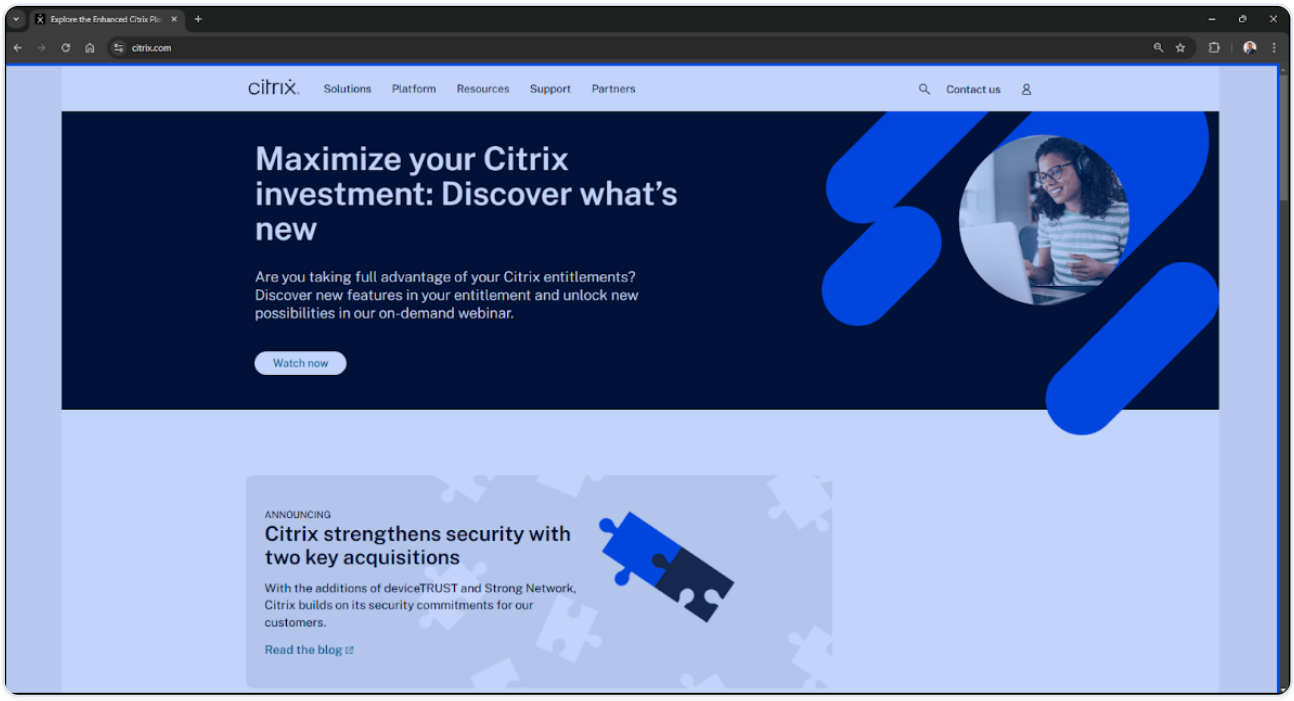
### Introdução

O Redirecionamento de Conteúdo do Navegador (BCR) melhora a experiência do usuário na navegação web em ambientes Citrix Virtual Apps and Desktops™. Ao descarregar a renderização de páginas web para a máquina local do usuário, o BCR reduz a carga do servidor e melhora o desempenho, especialmente para sites complexos ou que consomem muitos recursos.

### Como funciona

O BCR utiliza o aplicativo Citrix Workspace™ para criar um ambiente de navegação seguro no dispositivo do usuário. Quando um usuário acessa uma página web permitida, a viewport da janela do navegador é redirecionada para o cliente. O motor do navegador do lado do cliente então aproveita os recursos da máquina local para renderizar a página, resultando em tempos de carregamento mais rápidos e interação mais suave.

Observe que apenas a viewport do navegador é redirecionada. A viewport é a área retangular no seu navegador onde o conteúdo é exibido. A viewport não inclui itens como a Barra de Endereços, Barra de Favoritos ou Barra de Status. Esses itens estão na interface do usuário, que ainda está sendo executada no navegador no VDA.




## Principais Benefícios

O redirecionamento de conteúdo do navegador gerencia de forma inteligente o tráfego da web, proporcionando uma experiência superior para seus usuários enquanto reduz a carga sobre sua infraestrutura.

Veja como eles podem beneficiar sua organização:

- **Economia de Custos:** Descarregue páginas web que consomem muitos recursos para os dispositivos dos usuários, liberando recursos valiosos do servidor e reduzindo o consumo de largura de banda. Isso se traduz em custos de hardware e rede mais baixos.
- **Experiência do Usuário Aprimorada:** Ofereça aos seus usuários uma experiência de navegação mais suave e responsiva, mesmo com sites com muitos gráficos. Ofereça desempenho semelhante ao nativo, eliminando atrasos e melhorando a produtividade.
- **Segurança Aprimorada:** Mantenha um ambiente seguro enquanto permite o acesso a recursos internos e externos.
- **Flexibilidade Aumentada:** Suporte uma ampla gama de casos de uso, desde navegação web básica até aplicativos web complexos que exigem travessia de proxy ou autenticação SSO. Gerencie facilmente as configurações de redirecionamento com controles de política granulares no Citrix Web Studio™

# Requisitos do Sistema

## Componentes do lado do servidor

### Citrix Aplicativos Virtuais e Áreas de Trabalho

- Versão de Serviço de Longo Prazo
  - Requisitos mínimos - Qualquer versão LTSR do Citrix Virtual Apps and Desktops que não esteja no fim da vida útil
  - Recomendado - Citrix Virtual Apps and Desktops 2402 ou superior
- Versão Atual
  - Requisito mínimo - Qualquer versão CR do Citrix Virtual Apps and Desktops que não esteja no fim da vida útil
  - Recomendado - Versão mais recente do Citrix Virtual Apps and Desktops

### Componentes do Navegador

- Navegadores
  - Microsoft Edge
  - Google Chrome
- Extensão de redirecionamento do navegador: Publicada nas lojas da web do Chrome e do Edge
- Recomendamos usar a versão mais recente dos navegadores para a melhor experiência

> **Observação:**

> - Os links de extensão fornecidos acima estão geralmente disponíveis (GA) e são relevantes para implantações em nível de produção. Além das extensões GA, a Citrix também publica uma extensão Beta (GA + 1) especificamente na Google Chrome Store.
> - A Citrix recomenda que os clientes tenham usuários de teste na versão Beta para que as próximas atualizações sejam testadas e quaisquer problemas sejam relatados precocemente. Isso garante um processo tranquilo quando as extensões GA forem lançadas oficialmente.

- Os lançamentos de extensão geralmente correspondem aos lançamentos do Citrix Workspace App

## Componentes do lado do cliente

### Windows

- Windows 10 ou 11
- Citrix Workspace App
  - Requisito Mínimo - Qualquer Citrix Workspace App que não esteja no fim da vida útil
  - Recomendado
    - Long Term Service Release - Citrix Workspace App 2402 CU mais recente
    - Current Release - Citrix Workspace App 2405 ou superior

**Observação:**

- O redirecionamento de conteúdo do navegador não é compatível com as versões LTSR 1912 e 2203.1 do Citrix Workspace App para Windows.
- O mecanismo de navegador do lado do cliente necessário para o redirecionamento de conteúdo do navegador é instalado por padrão nas versões Current Releases do Citrix Workspace App.
- O mecanismo de navegador do lado do cliente necessário para o redirecionamento de conteúdo do navegador não é instalado por padrão na versão LTSR 2402 do Citrix Workspace App. Os administradores podem usar a opção ADDLOCAL para instalar os componentes do navegador BCR sobre o Citrix Workspace App.
- A partir do Citrix Workspace app 2507 para Windows, o Redirecionamento de Conteúdo do Navegador (BCR) é gerenciado como um componente modular, mas ainda é empacotado com o Citrix Workspace App. O componente BCR agora é instalado por padrão também nas versões LTSR, garantindo consistência entre CR e LTSR. Além disso, pacotes BCR autônomos serão publicados para situações que exigem atualizações independentes ou patches provisórios fora do ciclo de lançamento regular do Citrix Workspace app. Para mais detalhes, consulte a documentação do Citrix Workspace App para Windows.

Para mais detalhes, consulte documentação do Citrix Workspace App para Windows.

**Linux**

- Citrix Workspace App
  - Requisito mínimo - Qualquer Citrix Workspace App que não esteja no fim de vida útil
  - Recomendado - Citrix Workspace App 2408 ou superior Para mais detalhes, consulte a documentação do Citrix Workspace App para Linux

> **Observação:**

> - A partir do Citrix Workspace app 2601 para Linux, o Redirecionamento de Conteúdo do Navegador (BCR) é gerenciado como um componente modular. O componente BCR continua a ser empacotado e instalado por padrão com o Citrix Workspace app para Linux, garantindo uma experiência de usuário consistente. Além disso, pacotes BCR autônomos serão publicados para situações que exigem atualizações independentes ou patches provisórios fora do ciclo de lançamento regular do Citrix Workspace app. Para mais detalhes, consulte documentação do Citrix Workspace App para Linux

**ChromeOS**

- Citrix Workspace App
  - Versão mais recente da Chrome Web Store

**macOS**

- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma (até 14.2.1)
- Aplicativo Citrix Workspace
  - Requisito Mínimo - aplicativo Citrix Workspace 2411 ou superior

> **Observação:**

- Para macOS, o pacote de redirecionamento de conteúdo do navegador é independente do aplicativo Citrix Workspace e é sempre a versão mais recente. Assim, o pacote será compatível com várias versões do CWA acima da versão mínima especificada.
- Como não há dependência do aplicativo Citrix Workspace para Mac, a numeração da versão do Redirecionamento de Conteúdo do Navegador não corresponderá à versão do aplicativo Citrix Workspace para Mac.
- O mecanismo do navegador do lado do cliente não é empacotado com o aplicativo Citrix Workspace para Mac. Baixe e instale o lado do cliente para Mac em Citrix Downloads.
- Os pacotes Intel e ARM são separados. Assim, você precisa instalar a versão apropriada que se adapte ao endpoint do macOS.
- A partir do aplicativo Citrix Workspace 2511.1 para Mac, o componente Modular BCR é instalado por padrão, mas não é empacotado com o aplicativo Citrix Workspace, eliminando a necessidade de baixar e instalar manualmente o componente do Citrix Downloads. Pacotes BCR autônomos serão publicados para situações que exigem atualizações independentes ou patches provisórios fora do ciclo de lançamento regular do aplicativo Citrix Workspace. Para mais detalhes, consulte documentação do aplicativo Citrix Workspace para Mac.

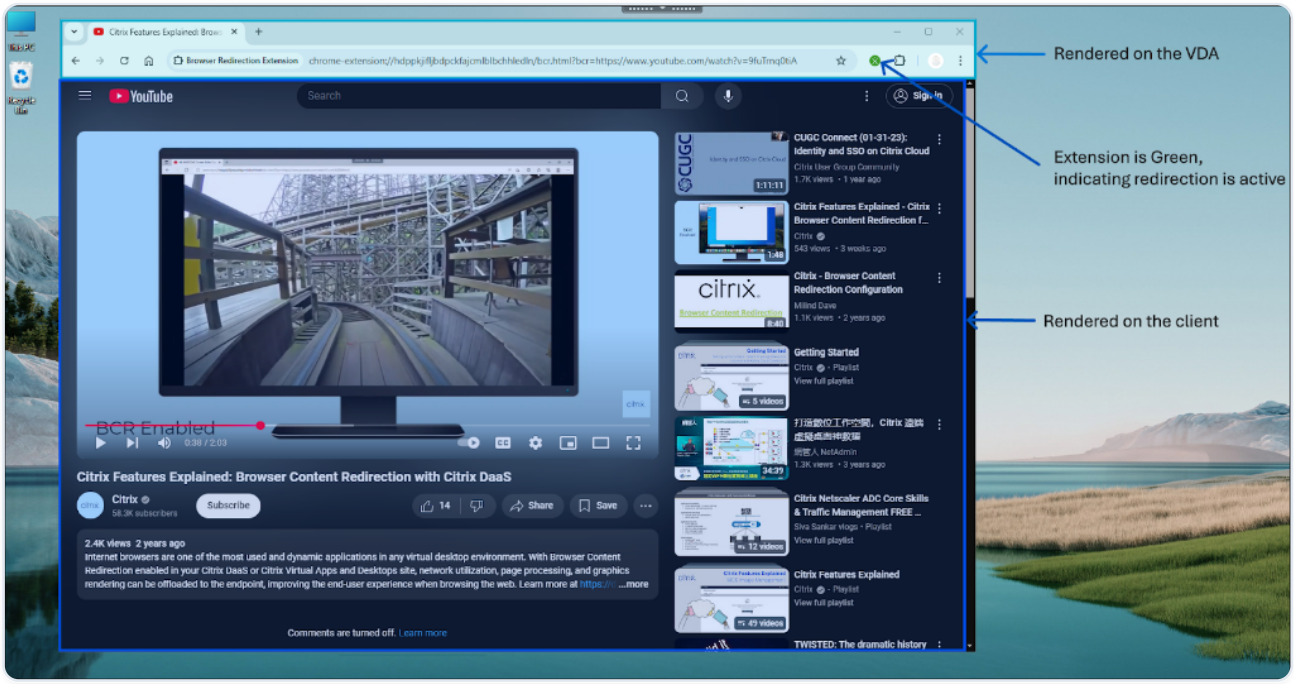
## Etapas para Configurar

1. Instale os componentes do lado do cliente e do lado do servidor de acordo com os requisitos do sistema.
    - Para detalhes sobre a implantação da extensão, consulte a seção Implantação da extensão.
2. Configurar as políticas do Studio
    - As políticas do Web Studio oferecem uma maneira granular de configurar o redirecionamento de conteúdo do navegador para se adequar a uma variedade de casos de uso
    - As políticas básicas permitem que o administrador configure URLs que precisam ser permitidas / não permitidas com o redirecionamento de conteúdo do navegador
    - As URLs podem ser configuradas com curingas
3. Abra um navegador da web compatível e navegar para uma URL permitida

- Se a correspondência for encontrada na lista de permissões, o site será redirecionado para o cliente
- O aplicativo Citrix Workspace combina a janela de visualização no navegador do lado do VDA para uma experiência perfeita

4. A cor do logotipo da extensão especifica o status do redirecionamento de conteúdo

- Verde: Ativo e Conectado
- Cinza: Não ativo / ocioso na guia atual
- Vermelho: Quebrado / Não Funcionando




**Observação:**

- O redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador são recursos independentes. As políticas de redirecionamento de vídeo HTML5 não são necessárias para que este recurso funcione. No entanto, o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX™ é usado para o redirecionamento de conteúdo do navegador.
- Recomendamos fazer todas as configurações através do Web Studio e não com chaves de registro.

# Opções de Configuração

A redireção de conteúdo do navegador oferece várias maneiras de configurar para se adequar aos casos de uso de diversos ambientes de clientes. Para obter informações detalhadas sobre as configurações de política, consulte Configurações de política de redirecionamento de conteúdo do navegador.

## Mecanismos de redirecionamento

### Busca pelo cliente, renderização pelo cliente

Por padrão, a redireção de conteúdo do navegador opera neste modo, ou seja, o mecanismo do navegador do lado do cliente acessa a página da web diretamente. Isso requer o acesso necessário da rede do cliente à página da web. O cenário de busca pelo cliente e renderização pelo cliente descarrega todo o uso de rede, CPU e RAM do Citrix VDA para o cliente e é a maneira mais otimizada de configurar a redireção de conteúdo do navegador.

#### OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Redirecionamento de conteúdo do navegador: Permitido
- Configuração de ACL de redirecionamento de conteúdo do navegador
  - Especifique os URLs que precisam ser redirecionados. Por padrão, o YouTube é o único site configurado para redirecionamento.
- Configuração da lista de bloqueio de redirecionamento de conteúdo do navegador
  - Opção de configuração opcional para bloquear quaisquer URLs/sub-URLs específicos do redirecionamento. Utilize esta opção com a anterior para obter o máximo de personalização.

### Busca pelo servidor, renderização pelo cliente

Neste caso, o mecanismo do navegador do lado do cliente contata e busca conteúdo do servidor web através do VDA usando um canal virtual. Esta opção é útil quando o cliente não tem acesso à internet (por exemplo, thin clients). Baixo consumo de CPU e RAM no VDA, mas a largura de banda é consumida no canal virtual ICA®.

Existem três modos de operação neste cenário. O termo proxy refere-se a um dispositivo proxy que o VDA acessa para obter acesso à Internet.

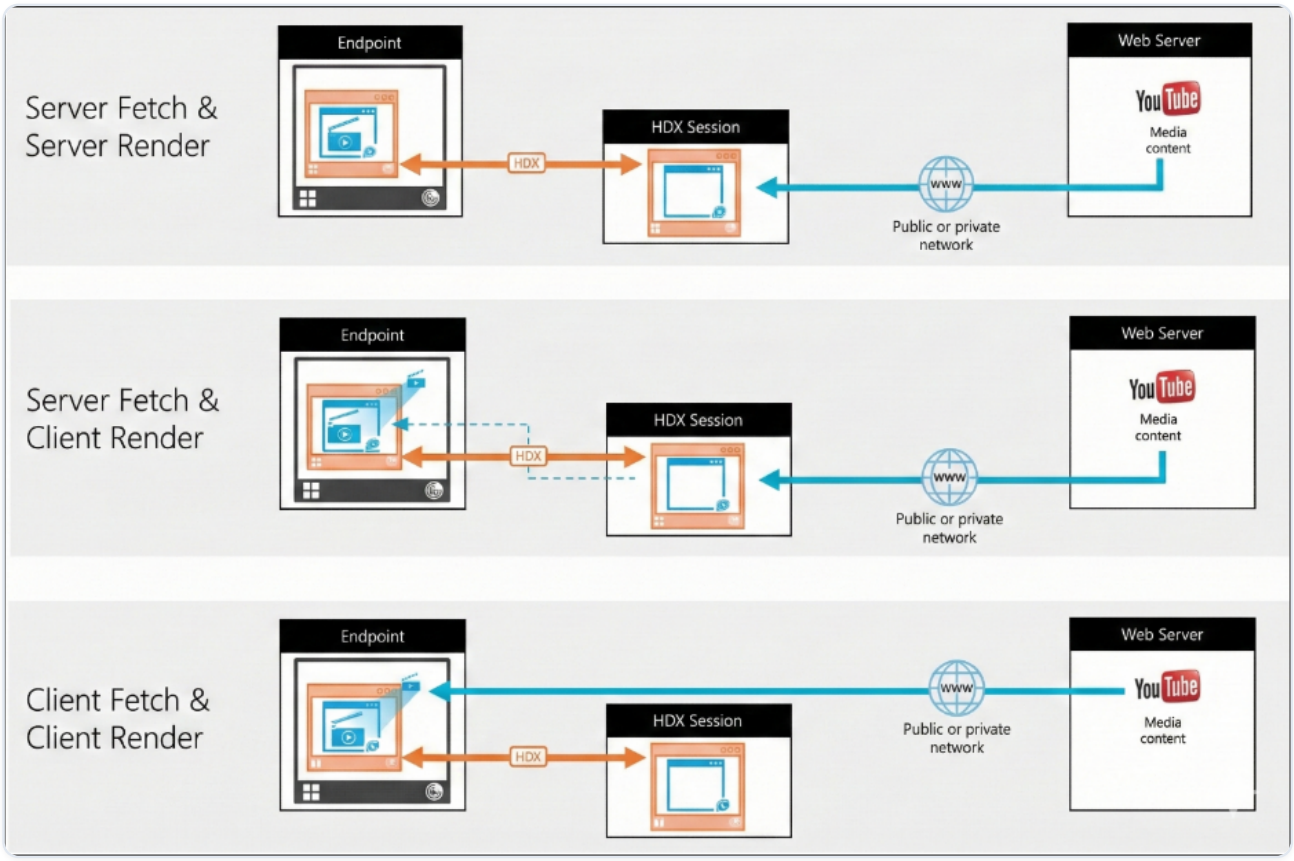
#### OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Além das políticas especificadas na seção Busca pelo cliente, renderização pelo cliente, configure o seguinte

- Configuração de proxy de redirecionamento de conteúdo do navegador
  - **Direto ou Transparente:** Configure isso se você quiser aproveitar a renderização do cliente com busca no servidor e tiver acesso direto ou acesso de proxy transparente à página da web a partir do VDA. A palavra-chave “DIRECT” deve ser configurada na política.
  - **Proxy Explícito:** Configure isso se você quiser aproveitar a renderização do cliente com busca no servidor e tiver acesso de proxy explícito à página da web a partir do VDA.
  - **Arquivos PAC:** Configure isso se você depender de arquivos PAC, os navegadores no VDA podem escolher automaticamente o servidor proxy apropriado para buscar uma URL especificada.

### Modo de fallback

Pode haver momentos em que o redirecionamento do cliente falha. Por exemplo, se a máquina cliente não tiver acesso direto à internet, uma resposta de erro pode ser enviada de volta ao VDA. Nesses casos, o navegador no VDA pode então recarregar e renderizar a página no servidor.



## Tratamento de autenticação

### Sites de autenticação

Na implementação atual do Redirecionamento de Conteúdo do Navegador, independentemente do mecanismo de redirecionamento, os sites de autenticação precisam ser configurados para que o Redirecionamento de Conteúdo do Navegador possa manipular o login em sites.

**Exemplo:**

1. Quando apenas `<https://www.youtube.com/>*` é configurado na configuração ACL de redirecionamento de conteúdo do navegador e nenhum site de autenticação é configurado, o BCR retornará à renderização do lado do servidor ao fazer login no site e continuará lá.
2. Neste caso, para que o BCR possa manipular sites de autenticação, configure `<https://www.accounts.google.com/>*` e quaisquer outros sites de autenticação, como o site IdP, conforme necessário. Cada login de site funciona de forma diferente e, portanto, certifique-se de listar
3. Quando configurado, o BCR irá manipular a autenticação. Por exemplo, com a renderização do cliente com busca no cliente - a autenticação também ocorrerá a partir do motor do navegador do lado do cliente para uma experiência de login perfeita.

#### OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

Configure a política de sites de autenticação de redirecionamento de conteúdo do navegador, além das políticas mencionadas na seção de mecanismos de redirecionamento

> **Observação:**
>
> - O navegador do lado do cliente do BCR não persiste cookies (incluindo autenticação) após o fechamento da janela redirecionada. Isso se manifestaria como a necessidade de fazer login novamente em sites quando as janelas do BCR são completamente fechadas e reabertas.
> - O navegador do lado do cliente do BCR não lê cookies do navegador do lado do VDA. Consequentemente, a personalização e as preferências do usuário não sincronizam com o navegador do VDA.

### Autenticação Integrada do Windows

O redirecionamento de conteúdo do navegador pode fornecer uma maneira contínua de autenticar para sites quando configurado com a Autenticação Integrada do Windows (IWA) dentro do mesmo domínio do VDA.

#### OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Configure a política de suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

Antes de habilitar o logon único, conclua o seguinte:

- Configure a infraestrutura Kerberos para emitir tickets para nomes de entidade de serviço (SPNs) construídos a partir do nome do host. Por exemplo, HTTP/serverhostname.com.
- Para renderização do cliente com busca no servidor: Ao usar o redirecionamento de conteúdo do navegador no modo de busca no servidor, certifique-se de que o DNS esteja configurado corretamente no VDA.
- Para renderização do cliente com busca no cliente: Ao usar o redirecionamento de conteúdo do navegador no modo de busca no cliente, certifique-se de que o DNS esteja configurado corretamente no dispositivo cliente e que você permita conexões TCP do overlay para o endereço IP do servidor web.

### Autenticação de Proxy

O redirecionamento de conteúdo do navegador pode fornecer uma maneira contínua de autenticar em seu proxy web ao buscar conteúdo do servidor. Quando habilitado, o Redirecionamento de Conteúdo do Navegador obterá e usará automaticamente um ticket de serviço Kerberos para autenticar com o proxy.

#### OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Configure a política de autenticação de proxy de busca no servidor para redirecionamento de conteúdo do navegador

Antes de habilitar a política de autenticação de proxy de busca no servidor, conclua o seguinte:

- Você precisa configurar seu arquivo PAC para rotear o tráfego através de um proxy web downstream e configurar o proxy para usar a autenticação Kerberos

## Casos de Uso

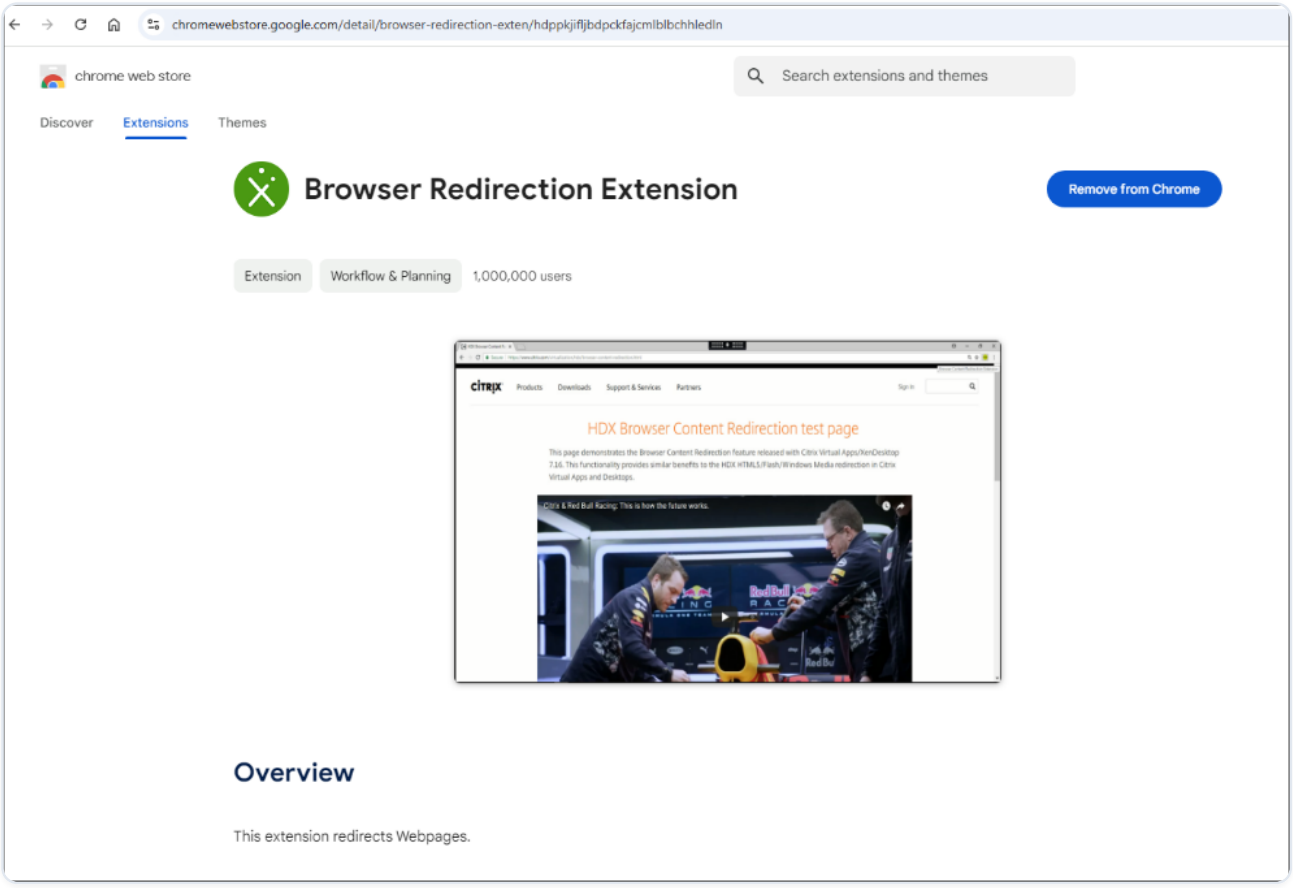
A Redireção de Conteúdo do Navegador (BCR) pode ser utilizada para uma ampla gama de sites, particularmente aqueles que consomem muitos recursos e são frequentemente acessados por

empresas. Isso inclui plataformas de streaming de vídeo como o YouTube, que podem se beneficiar significativamente do descarregamento da renderização para dispositivos de endpoint, reduzindo assim a carga do servidor e economizando custos. Além disso, o BCR é ideal para aplicativos de comunicações unificadas, como ferramentas de videoconferência e colaboração (Google Meet, Teams web, Zoom web) e aplicativos de contact center (Genesys cloud), garantindo desempenho suave e experiência do usuário aprimorada. Ao aproveitar o BCR, as empresas podem otimizar seus recursos e melhorar a eficiência em vários aplicativos baseados na web. Consulte CTX238236 para obter informações sobre como configurar sites específicos.

## Implantação da Extensão

### Implantar Manualmente

A extensão de redirecionamento do navegador é publicada nas lojas da web do Chrome e Edge. A extensão é necessária apenas no navegador no VDA e não no lado do cliente. Para instalar a extensão, navegar até a webstore do Chrome / Edge, procure pela extensão de redirecionamento do navegador e adicione-a aos respectivos navegadores. Este método funciona para usuários individuais. Para implantar a extensão para um grande grupo de usuários, implante a extensão usando a política de grupo



### Implantar Usando a Política de Grupo

#### PRÉ-REQUISITOS

- **Acesso:** Você precisará de privilégios de administrador na máquina ou dentro do seu ambiente do Active Directory onde você configurará a Política de Grupo.
- **Arquivos ADMX:** Baixe os arquivos ADMX do Google Chrome (modelos administrativos) para sua versão do Chrome. Você pode encontrá-los na página Google Chrome Enterprise Help.
- **Modelos do Edge:** Baixe os modelos administrativos do Microsoft Edge (arquivos ADMX) na página Microsoft Edge Enterprise.
- **ID da Extensão e URL de Atualização:** A ID da extensão e a URL de atualização para a extensão de Redirecionamento de Conteúdo do Navegador Citrix.

#### ETAPAS PARA O GOOGLE CHROME

1. Importar Arquivos ADMX:
    - Copie os arquivos ADMX do Chrome para seu armazenamento central de modelos administrativos. Isso geralmente é %SystemRoot%\PolicyDefinitions no seu controlador de domínio.
2. Abrir Gerenciamento de Política de Grupo:
    - Inicie o Console de Gerenciamento de Política de Grupo (gpmc.msc).
3. Criar ou Editar um GPO:
    - Crie um novo Objeto de Política de Grupo (GPO) ou edite um existente que se aplique aos usuários ou computadores onde você deseja implantar a extensão.
4. navegar até as Configurações de Extensões:
    - No editor de GPO, vá para:
        - Configuração do Usuário > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Google > Google Chrome > Extensões
5. Habilite "Configurar a lista de aplicativos e extensões instalados à força":
    - Dê um duplo clique nesta configuração de política e selecione "Habilitado".
    - Se a configuração "Configurar a lista de aplicativos e extensões instalados à força" estiver definida como Desabilitado, a extensão será automaticamente removida do Chrome para todos os usuários.

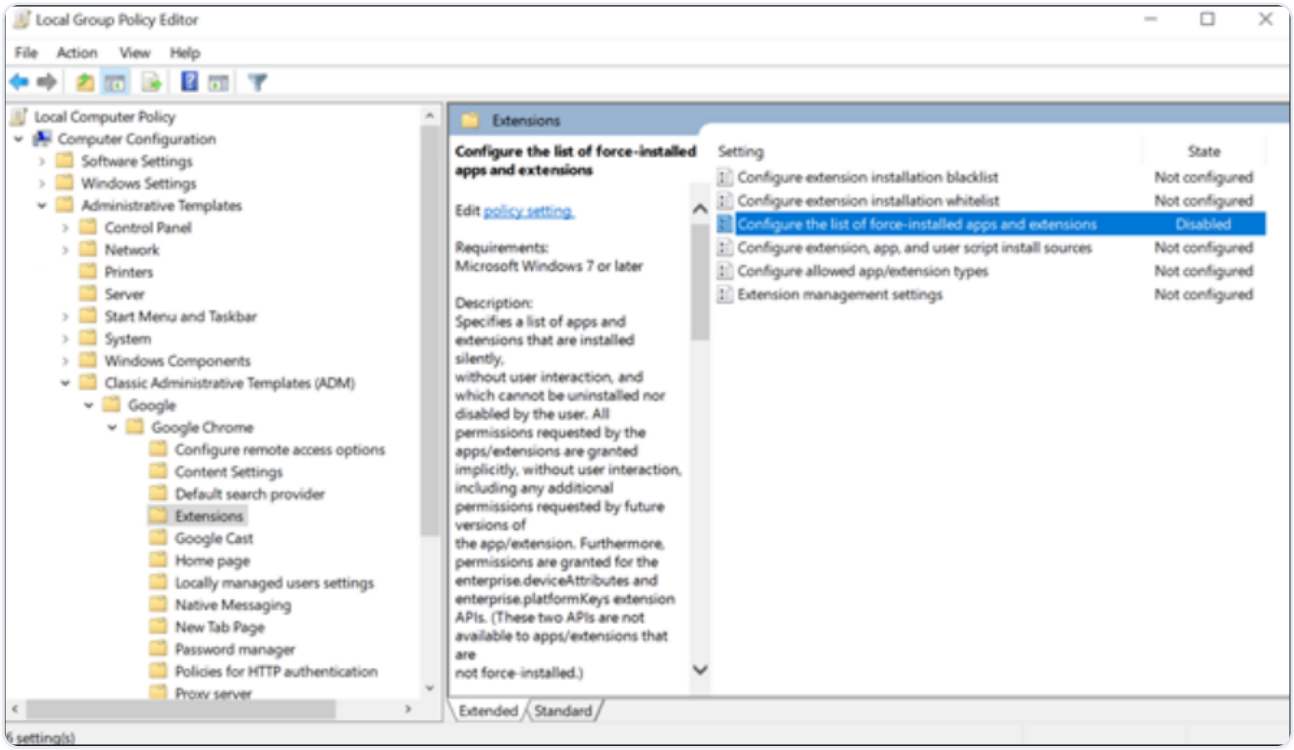
6. Adicione o ID da Extensão e o URL de Atualização:
    - Clique no botão "Mostrar".
    - Insira o ID da extensão e o URL de atualização no formato: <extension_id>;<update_url>
    - Valor: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx>` (URL de Atualização)
7. Aplique o GPO:
    - Vincule o GPO à Unidade Organizacional (OU) apropriada em sua estrutura do Active Directory.
8. Atualizar Política de Grupo:
    - Nas máquinas de destino, execute gpupdate /force para aplicar a política imediatamente ou aguarde a atualização automática da política.

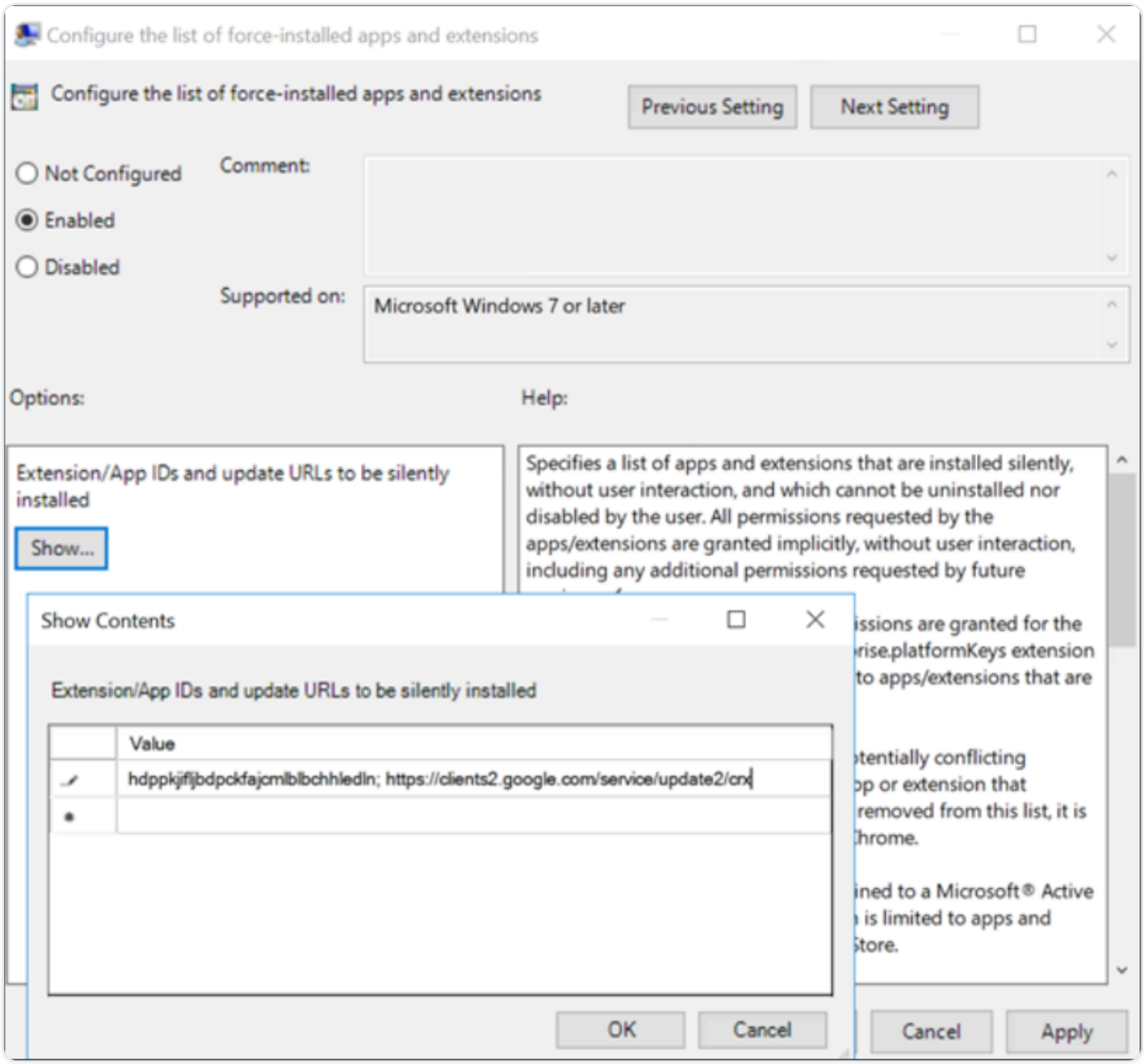
### ETAPAS PARA O MICROSOFT EDGE

1. Importar Arquivos ADMX:
    - Copie os arquivos ADMX do Edge para seu armazenamento central de modelos administrativos (%SystemRoot%\PolicyDefinitions).
2. Abrir Gerenciamento de Política de Grupo:
    - Inicie o Console de Gerenciamento de Política de Grupo (gpmc.msc).
3. Criar ou Editar um GPO:
    - Crie um novo GPO ou edite um existente.
4. navegar para Configurações de Extensões:
    - No editor de GPO, vá para:
        - Configuração do Computador > Políticas > Modelos Administrativos > Microsoft Edge > Extensões
5. Habilitar "Controlar quais extensões são instaladas silenciosamente":
    - Clique duas vezes nesta configuração de política e selecione "Habilitado".
6. Adicionar o ID da Extensão e a URL de Atualização:
    - Clique no botão "Mostrar".

- Insira o ID da extensão e a URL de atualização no formato: <extension_id>;<update_url>
- Valor: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx>` (URL de atualização)

7. Aplicar o GPO:
   - Vincule o GPO à Unidade Organizacional (OU) apropriada em sua estrutura do Active Directory.
8. Atualizar a Política de Grupo:
   - Nas máquinas de destino, execute gpupdate /force ou aguarde a atualização automática.






## Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo da central de conhecimento Como solucionar problemas de redirecionamento de conteúdo do navegador.

## Limitações do Redirecionamento de Conteúdo do Navegador

### Limitações do lado do servidor (VDA)

O redirecionamento de conteúdo do navegador não pode suportar os seguintes casos de uso. Caso seja necessário um aprimoramento para qualquer um dos cenários mencionados ou novos cenários, entre em contato com a equipe de produto da Citrix.

- Janelas pop-up não são suportadas com o redirecionamento de conteúdo do navegador.
- A persistência de cookies de sessão não é suportada.

- A política de redirecionamento de vídeo HTML5 deve ser desativada quando o redirecionamento de conteúdo do navegador estiver em uso.
- Em cenários de desconexão/reconexão de sessão, a janela do navegador VDA precisa ser atualizada para que o BCR seja ativado novamente.
- Impressão e downloads de arquivos de janelas com BCR não são suportados.
- O modo de navegação anônima ou privada não é suportado com o redirecionamento de conteúdo do navegador.

### Limitações do lado do cliente (CWA)

- O redirecionamento de conteúdo do navegador não é suportado na estrutura ARMhf.
- O BCR suporta um máximo de 25 guias redirecionadas em um navegador e um total de 30 guias redirecionadas em dois navegadores.

# Videoconferência HDX™ e compactação de vídeo de webcam

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

> Webcams podem ser usadas por aplicativos em execução na sessão virtual usando a compactação de vídeo de webcam HDX ou o redirecionamento USB genérico plug-n-play HDX. Use **Citrix Workspace™ app > Preferências > Dispositivos** para alternar entre os modos. A Citrix recomenda que você sempre use a compactação de vídeo de webcam HDX, se possível. O redirecionamento USB genérico HDX é recomendado apenas quando há problemas de compatibilidade de aplicativos com a compactação de vídeo HDX ou quando você precisa de funcionalidades nativas avançadas da webcam. Para melhor desempenho, a Citrix recomenda que o Virtual Delivery Agent tenha pelo menos duas CPUs virtuais.

Para impedir que os usuários alternem da compactação de vídeo de webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em **Configurações de política ICA® > Configurações de política de dispositivos USB**. Os usuários do Citrix

Workspace app podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**.

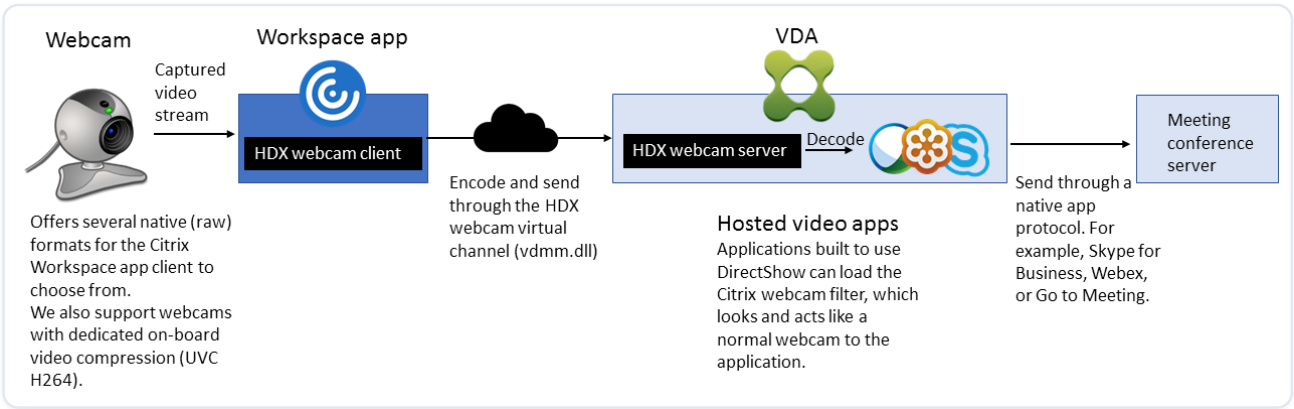
## Compressão de vídeo de webcam HDX

A compactação de vídeo de webcam HDX também é chamada de modo de webcam **Otimizado**. Esse tipo de compactação de vídeo de webcam envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compactação de webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Esse recurso é habilitado por padrão.

Para desabilitar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina a chave do registro como 0 no VDA. Para obter informações, consulte Compactação de vídeo de webcam na lista de recursos gerenciados por meio do registro.

Se você desabilitar a funcionalidade padrão para streaming de recursos de vídeo, a compactação de vídeo de webcam HDX usará a tecnologia de framework multimídia que faz parte do sistema operacional cliente para interceptar o vídeo de dispositivos de captura, transcodificá-lo e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do SO.

O cliente lida com a comunicação com a webcam. O cliente então envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua integração oferece a mesma experiência em sua área de trabalho. O aplicativo Workspace compacta o vídeo para economizar largura de banda e fornecer melhor resiliência em cenários de WAN.




A política de **Conferência multimídia** deve estar habilitada para a compactação de vídeo de webcam HDX. Essa política é habilitada por padrão.

Se uma webcam suportar codificação de hardware, a compressão de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de

banda do que a codificação de software. Para forçar a compressão de software, edite a chave do registro no cliente. Para obter informações, consulte Compressão de software de webcam na lista de recursos gerenciados através do registro.

### Requisitos de compressão de vídeo de webcam HDX

A compressão de vídeo de webcam HDX suporta as seguintes versões do aplicativo Citrix Workspace:

| PLATAFORMA | PROCESSADOR |
|---|---|
| Aplicativo Citrix Workspace para Windows | O aplicativo Citrix Workspace para Windows oferece suporte à compactação de vídeo de webcam para aplicativos de 32 bits e 64 bits no XenApp e XenDesktop 7.17 e posterior. Em versões anteriores, o aplicativo Citrix Workspace para Windows oferece suporte apenas a aplicativos de 32 bits. |
| Aplicativo Citrix Workspace para Mac | O aplicativo Citrix Workspace para Mac 2006 ou posterior oferece suporte à compactação de vídeo de webcam para aplicativos de 64 bits no XenApp e XenDesktop 7.17 e posterior. Em versões anteriores, o aplicativo Citrix Workspace para Mac oferece suporte apenas a aplicativos de 32 bits. |
| Aplicativo Citrix Workspace para Linux | O aplicativo Citrix Workspace para Linux oferece suporte a aplicativos de 32 bits e 64 bits no desktop virtual. |
| Aplicativo Citrix Workspace para Chrome | Como alguns Chromebooks ARM não oferecem suporte à codificação H.264, apenas aplicativos de 32 bits podem usar a compactação de vídeo de webcam HDX otimizada. |

Aplicativos de vídeo baseados em Media Foundation oferecem suporte à compactação de vídeo de webcam HDX no Windows 8.x ou superior e Windows Server 2012 R2 e superior. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.
- Webcam compatível com DirectShow (use as configurações padrão da webcam). Webcams com capacidade de codificação de hardware reduzem o uso da CPU do lado do cliente.
- Para a compactação de vídeo de webcam HDX, instale os drivers da webcam no cliente, obtidos do fabricante da câmera, se possível. A instalação dos drivers do dispositivo não é necessária no servidor.

Diferentes webcams oferecem diferentes taxas de quadros e têm diferentes níveis de brilho e contraste. Ajustar o contraste da webcam pode reduzir significativamente o tráfego de upstream. A Citrix usa as seguintes webcams para a validação inicial dos recursos:

- Modelos Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar a taxa de quadros de vídeo preferida, edite a chave do registro no cliente. Para obter informações, consulte Taxa de quadros de compressão de vídeo da webcam na lista de recursos gerenciados através do registro.

## Streaming de webcam de alta definição

O aplicativo de videoconferência no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo. Quando a webcam e o aplicativo de videoconferência suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos todas as resoluções de webcam.

Este recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver para Windows, versão mínima 4.10.

Você pode usar uma chave do registro para desabilitar e habilitar o recurso. Para obter informações, consulte Streaming de webcam de alta definição na lista de recursos gerenciados através do registro.

Se a negociação do tipo de mídia falhar, o HDX retorna à resolução VGA padrão (640 x 480 pixels). Você pode usar chaves do registro no cliente para configurar a resolução padrão.

Certifique-se de que a câmera suporte a resolução especificada. Para obter informações, consulte Resolução de webcam de alta definição na lista de recursos gerenciados através do registro.

A compressão de vídeo da webcam HDX usa significativamente menos largura de banda em comparação com o redirecionamento USB genérico plug-n-play e funciona bem em conexões WAN. Para ajustar a largura de banda, defina a chave do registro no cliente. Para obter informações, consulte Largura de banda da webcam de alta definição na lista de recursos gerenciados através do registro.

Insira um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usarão 350000 bps por padrão.

### Redirecionamento USB genérico plug-n-play do HDX

O redirecionamento USB genérico plug-n-play HDX (isócrono) também é chamado de modo de webcam **Genérico**. O benefício do redirecionamento USB genérico plug-n-play HDX é que você não precisa instalar drivers em seu thin client/endpoint. A pilha USB é virtualizada de forma que qualquer coisa que você conecte ao cliente local é enviada para a VM remota. A área de trabalho remota age como se você a tivesse conectado nativamente. A área de trabalho do Windows lida com toda a interação com o hardware e executa a lógica plug-n-play para encontrar os drivers corretos. A maioria das webcams funciona se os drivers existirem no servidor e puderem funcionar via ICA. O modo de webcam genérico usa significativamente mais largura de banda (muitos Megabits por segundo) porque você está enviando vídeo não compactado com o protocolo USB pela rede.

## Redirecionamento multimídia HTML5

O redirecionamento multimídia HTML5 estende os recursos de redirecionamento multimídia do HDX™ MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento na distribuição online de conteúdo multimídia, especialmente para dispositivos móveis, a indústria de navegadores desenvolveu maneiras mais eficientes de apresentar áudio e vídeo.

O Flash tem sido o padrão, mas requer um plug-in, não funciona em todos os dispositivos e tem um consumo de bateria maior em dispositivos móveis. Empresas como YouTube, Netflix e versões mais recentes de navegadores da Mozilla, Google e Microsoft estão migrando para o HTML5, tornando-o o novo padrão.

A multimídia baseada em HTML5 tem muitas vantagens sobre plug-ins proprietários, incluindo:

- Padrões independentes de empresas (W3C)

- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança levantados pelos plug-ins

## Downloads progressivos HTTP

O download progressivo HTTP é um método de pseudo-streaming baseado em HTTP que suporta HTML5. Em um download progressivo, o navegador reproduz um único arquivo (codificado em uma única qualidade) enquanto ele está sendo baixado de um servidor web HTTP. O vídeo é armazenado na unidade à medida que é recebido e é reproduzido da unidade. Se você assistir ao vídeo novamente, o navegador pode carregar o vídeo do cache.

Para um exemplo de download progressivo, consulte a página de teste de redirecionamento de vídeo HTML5. Para inspecionar os elementos de vídeo na página da web e encontrar as fontes (formato de contêiner mp4) nas tags de vídeo HTML5, use as ferramentas de desenvolvedor em seu navegador:

## Comparando HTML5 e Flash

| RECURSO | HTML5 | FLASH |
|---|---|---|
| Requer um reprodutor proprietário | Não | Sim |
| Executa em dispositivos móveis | Sim | Alguns |
| Velocidade de execução em diferentes plataformas | Alta | Lento |
| Compatível com iOS | Sim | Não |
| Uso de recursos | Menos | Mais |
| Carrega mais rápido | Sim | Não |

## Requisitos

Oferecemos suporte apenas para redirecionamento de downloads progressivos no formato mp4. Não oferecemos suporte a WebM e tecnologias de streaming de taxa de bits adaptável como DASH/HLS.

Suportamos o seguinte e usamos políticas para controlá-los. Para obter mais informações, consulte Configurações de política de multimídia.

- Renderização do lado do servidor
- Busca do servidor, renderização do cliente
- Busca e renderização do lado do cliente

Versões mínimas do aplicativo Citrix Workspace™ e do Citrix Receiver™:

- Citrix Workspace app 1808 para Windows
- Citrix Receiver para Windows 4.5
- Citrix Workspace app 1808 para Linux
- Citrix Receiver para Linux 13.5

| VERSÃO MÍNIMA DO NAVEGADOR VDA | VERSÃO/COMPILAÇÃO/SP DO SO WINDOWS |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Firefox 47 Adicione manualmente os certificados ao armazenamento de certificados do Firefox ou configure o Firefox para procurar certificados em um armazenamento de certificados confiável do Windows. Para obter mais informações, consulte `https://wiki.mozilla.org/CA:AddRootToFirefox` | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Chrome 51 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |

## Componentes da solução de redirecionamento de vídeo HTML5

- **HdxVideo.js** - Hook JavaScript que intercepta comandos de vídeo no site. HdxVideo.js se comunica com o WebSocketService usando WebSockets Seguros (SSL/TLS).
- **Certificados SSL do WebSocket**

  - Para a CA (raiz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) Localização: **Certificados (Computador Local) > Autoridades de Certificação Raiz Confiáveis > Certificados**.
  - Para a entidade final (folha): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) Localização: **Certificados (Computador Local) > Pessoal > Certificados**.

- **WebSocketService.exe** - Executa no sistema local e realiza a terminação SSL e o mapeamento da sessão do usuário. WebSocket Seguro TLS escutando em 127.0.0.1 porta 9001.
- **WebSocketAgent.exe** - Executa na sessão do usuário e renderiza o vídeo conforme instruído pelos comandos do WebSocketService.

## Como faço para habilitar o redirecionamento de vídeo HTML5?

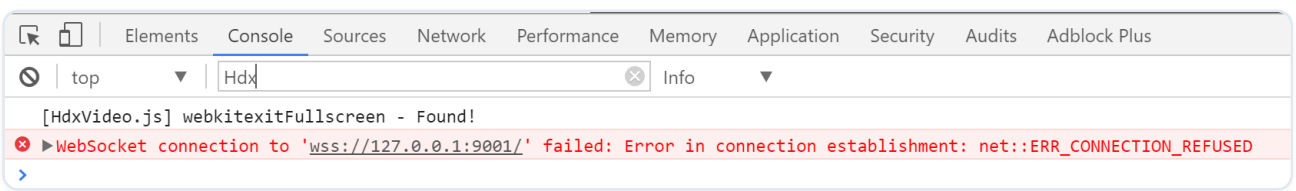
Nesta versão, este recurso está disponível apenas para páginas da web controladas. Requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas da web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de Taxa de Bits Adaptativa (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não são suportados.

Para obter mais informações, consulte *Configurações de política de multimídia*.

## Dicas de Solução de Problemas

Podem ocorrer erros quando a página da web tenta executar HdxVideo.js. Se o JavaScript falhar ao carregar, o mecanismo de redirecionamento HTML5 falhará. Certifique-se de que não há erros relacionados a HdxVideo.js inspecionando o console nas janelas da ferramenta de desenvolvedor do seu navegador. Por exemplo:



# Otimização para Microsoft Teams (Novo)

A Citrix® oferece suporte a duas formas de otimizar o áudio e vídeo do Microsoft Teams em um ambiente VDI: Otimização Citrix HDX™ e a Nova solução VDI para Teams da Microsoft. O Teams Clássico chegou ao fim da vida útil, portanto, as abordagens de otimização descritas nesta página se aplicam ao cliente atual do Microsoft Teams.

> **Observação:**
>
> A Microsoft anunciou a descontinuação da Otimização Citrix HDX baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:
>
> - October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.
> - April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.
>
> Recomenda-se que os clientes migrem para a Nova solução VDI para Teams. Essa alteração afeta apenas os endpoints Windows. Endpoints macOS, Linux, ChromeOS e HTML5 não são afetados. Para obter mais detalhes, consulte Blog da Microsoft.

## Abordagens de otimização

- **Otimização Citrix HDX (MTOP)**: Uma solução combinada da Citrix e da Microsoft que usa um canal virtual de propriedade da Citrix (CTXMTOP). O descarregamento de mídia é tratado por `HdxRtcEngine` no aplicativo Citrix Workspace™. Essa solução é tradicionalmente conhecida como MTOP.
- **Nova solução VDI para Teams**: Uma otimização mais recente que é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2). Está disponível em endpoints Windows e Mac. Para obter detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.

## Principais distinções

| OTIMIZAÇÃO CITRIX HDX | NOVA SOLUÇÃO VDI PARA TEAMS |
|---|---|
| A otimização é uma solução combinada da Citrix e da Microsoft e usa um canal virtual de propriedade da Citrix (CTXMTOP). | A solução de otimização é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2). |
| O descarregamento de mídia é tratado por `HdxRtcEngine` que reside no aplicativo Citrix Workspace. | O descarregamento de mídia é tratado pelo mecanismo de mídia SlimCore em endpoints Windows e Mac. |
| Nenhum componente adicional é necessário no endpoint, exceto a instalação do aplicativo Citrix Workspace. | Um componente adicional - o **Teams VDI Plugin** - precisa ser implantado no endpoint por vários meios. Este plug-in gerencia o download e as atualizações do mecanismo de mídia SlimCore. |
| Disponível nas plataformas de endpoint - Windows, macOS, Linux e ChromeOS. | Disponível nas plataformas de endpoint - Windows e Mac. |
| Novos recursos são gerenciados em conjunto entre a Citrix e a Microsoft. | Novos recursos são gerenciados pela Microsoft. Os usuários têm acesso a alguns novos recursos indisponíveis com a Otimização Citrix HDX. |
| Suportado tanto pela Citrix quanto pela Microsoft, dependendo do componente envolvido. Os clientes podem abrir um caso com a Citrix ou com a Microsoft e são redirecionados para a equipe apropriada conforme necessário. | De propriedade e suportado pela Microsoft. A Citrix oferece suporte aos componentes Citrix envolvidos, como o aplicativo Citrix Workspace, a lista de permissões do canal virtual e os mecanismos de implantação de plug-ins. |

## Interoperabilidade e roaming

A Otimização Citrix HDX e a nova solução VDI para Teams podem coexistir, mas o cliente Teams usa apenas uma delas por vez.

- A otimização é selecionada quando o aplicativo Teams é iniciado, na seguinte ordem: nova solução VDI para Teams, depois Otimização Citrix HDX (WebRTC), depois redirecionamento padrão de áudio/vídeo.

- Se a nova solução VDI para Teams falhar, o Teams retorna diretamente para o redirecionamento padrão de áudio/vídeo, em vez de para o WebRTC. É necessário reiniciar o aplicativo Teams para executar novamente a seleção e escolher a otimização adequada.
- O roaming entre endpoints é contínuo e não requer a reinicialização do aplicativo Teams, inclusive quando um usuário faz roaming entre um endpoint que suporta a nova solução VDI para Teams e um que não suporta.

## Otimização Citrix HDX™

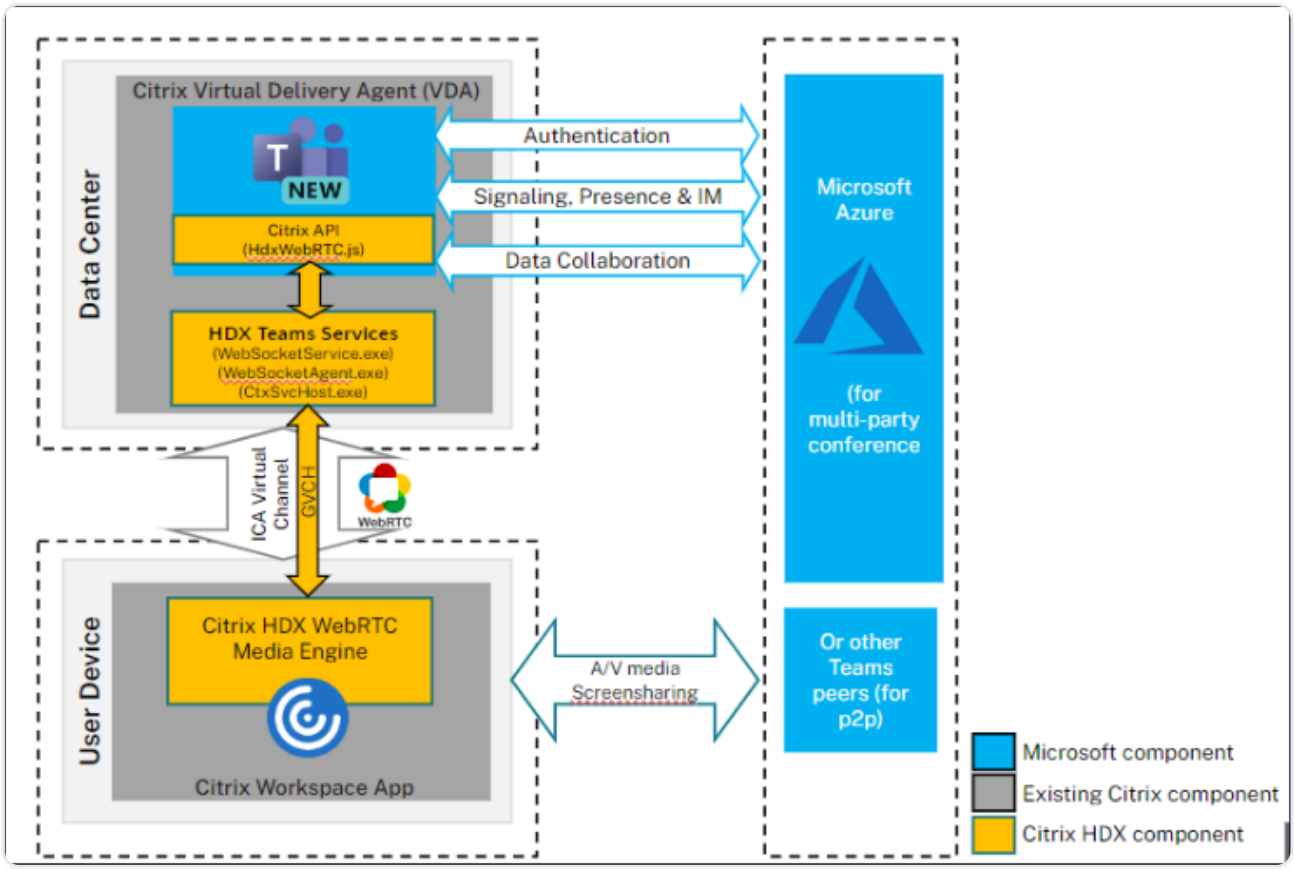
**Observação:**

A Microsoft anunciou a descontinuação da Otimização HDX baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

- October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix
- April 1, 2027 - Fim da Disponibilidade: A Microsoft anunciou a descontinuação da Otimização HDX WebRTC para endpoints Windows. A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

Recomenda-se que os clientes migrem para a nova solução VDI para Microsoft Teams (SlimCore). Essa mudança afeta apenas os endpoints Windows — os endpoints macOS, Linux, ChromeOS e HTML5 não são impactados. Para mais detalhes, consulte o Blog da Microsoft.

No Citrix HDX (Otimização WebRTC), o mecanismo de mídia (HdxRtcEngine) no endpoint responsável pelo tratamento da mídia descarregada é incorporado ao aplicativo Citrix Workspace™ e a instalação do aplicativo Citrix Workspace instala automaticamente o mecanismo também.




## Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para suportar o novo cliente Teams. Observe que, nas versões mínimas, algumas correções de bugs críticas ou os recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as últimas correções e recursos.

### Sistemas operacionais VDI

Para informações detalhadas, consulte as recomendações fornecidas na documentação da Microsoft.

**Observação:**

- O Windows Server 2016 não é suportado. A Citrix recomenda que você planeje suas atualizações de acordo.
- Como as versões são atualizadas frequentemente, as versões mencionadas aqui podem se tornar obsoletas (end-of-life). Portanto, consulte as páginas de ciclo de vida do produto do aplicativo Citrix Workspace e do Citrix Virtual Apps and Desktops para garantir que você esteja usando versões suportadas de diferentes componentes.

- Se você estiver usando o Citrix Virtual Apps and Desktops™ 1912 LTSR, a Citrix recomenda planejar uma atualização, pois ele chegará ao fim da vida útil em dezembro de 2024.

### Virtual Delivery Agent (VDA)

| VERSÕES MÍNIMAS | VERSÕES RECOMENDADAS |
|---|---|
| 1912 LTSR CU8+; 2203 LTSR (qualquer CU); 2212 CR | 2203 LTSR CU5+ (ou) 2402 LTSR e quaisquer versões CR acima |

### Aplicativo Citrix Workspace

| VERSÕES MÍNIMAS | VERSÕES RECOMENDADAS |
|---|---|
| Windows 2203 LTSR (CU mais recente); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301 | Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405 |

## Implantação

1. Instale o novo cliente Teams no VDI. Para obter informações detalhadas, consulte Implantar o novo Teams para VDI.
2. Configure a seguinte chave de registro no VDA para otimizar o novo Teams.
   - **Local**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **Chave (REG_Multi_SZ)**: `ProcessWhitelist`
   - **Valor**: `msedgewebview2.exe`

   **Observação:**

   A partir do Citrix Virtual Apps and Desktops 2402 LTSR (ou) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, você não precisa configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela é permitida por padrão.
3. Certifique-se de que a política Redirecionamento do Microsoft Teams esteja ativada. Esta política é ativada por padrão.

4. Nenhuma configuração adicional é necessária no lado do cliente. Siga as instruções do assistente para instalar o aplicativo Citrix Workspace.

#### App Layering

O novo Microsoft Teams mudou seu método de instalação e agora é instalado em C:\Program Files\WindowsApps. Para suportar essa mudança, você deve executar o App Layering versão 2403.2 ou posterior. Você pode baixar um disco de atualização na página Downloads do App Layering que inclui esta correção.

Para obter informações detalhadas, consulte a documentação do App Layering.

#### Citrix Profile Management

Consulte a documentação Citrix Profile Management para obter informações sobre como habilitar o roaming para o Novo Microsoft Teams. A orientação de versão mínima atual para o Citrix Profile Management é 2402 LTSR (ou) 2203 LTSR CU5+.

### Considerações de rede

Os requisitos de rede para o novo Teams não diferem do Teams Clássico. Portanto, consulte a seção Requisito de Rede na documentação do Teams Clássico.

### Matriz de recursos e suporte de versão

Como as versões são atualizadas frequentemente, algumas versões mais antigas mencionadas aqui podem atingir o fim da vida útil. Portanto, consulte as páginas de ciclo de vida do produto de Citrix Workspace App e Citrix Virtual Apps and Desktops para garantir que você esteja usando versões compatíveis de diferentes componentes.

> **Observação:**
>
> - As versões mencionadas aqui são as versões mínimas a partir das quais o recurso específico é suportado (ou) a versão mínima na qual o Novo Teams é suportado, o que for maior.
> - O Citrix Virtual Apps and Desktops 1912 LTSR CU8+ mencionado na seção de versões mínimas não está sendo citado na tabela abaixo, pois atingirá o fim de sua vida útil em dezembro de 2024. No entanto, ainda é uma versão suportada até lá.
> - Recursos que têm as versões mínimas do Citrix Virtual Apps and Desktops como `N/A` apenas implicam que o recurso não envolveu nenhuma alteração do lado do VDA.

| RECURSO | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|
| Áudio / Vídeo (p2p e conferência) | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2301 |
| Compartilhamento de tela | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2301 |
| i. Borda Vermelha do Indicador de Tela | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | Não |
| ii. Limitar a captura ao Desktop Viewer | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | Não |
| iii. Vários monitores | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | Não |
| DTMF | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2301 |

| RECURSO | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|
| Suporte a Servidor Proxy | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2305 |
| Compartilhamento de apps | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2209 | Não |
| Legendas ao Vivo | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2303 |
| e911 Dinâmico | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2301 |
| Conceder Controle | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | Não |
| Solicitar Controle | N/A | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2303 |
| Múltiplas Janelas | 2203 LTSR (qualquer | 2203 LTSR CU mais | 2302 | 2207 | 2303 |

| RECURSO | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|
| | CU), 2212 CR | recente, 2302 CR | | | |
| Transcrições de Reunião | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2207 | 2303 |
| Desfoque de plano de fundo | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR | 2302 | 2212 | 2303 |
| Compartilhamento de tela (com Proteção de Aplicativos) | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2309.1 CR | 2308 | 2311 | Não |
| Simulcast | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2305 CR | 2305 | 2305 | 2312 |
| Campainha Secundária | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2307.1 CR | 2308 | 2308 | 2312 |
| Compartilhar Áudio do Sistema | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2403 CR | 2405 | 2402 | Não |

## Solução de problemas e outras considerações

Para o New Teams, consulte CTX253754 , Solução de problemas do Microsoft Teams. Para as atualizações mais recentes sobre qualquer coisa relacionada ao New Teams, consulte CTX585013.

## Limitações conhecidas

### Limitações no aplicativo Citrix Workspace

- Suporte HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo pode ser capturado.
- Limitações de compartilhamento de áudio do sistema
  - O áudio não pode ser compartilhado usando este recurso ao compartilhar a tela com aplicativos ou guias redirecionados RAVE e BCR.
  - Este recurso é suportado apenas em desktops publicados

### Limitações no VDA

- O novo Teams como um aplicativo publicado (seamless) não é suportado
  - Corrigido no CVAD 2402 LTSR, 2203 LTSR CU5 e superior
- Quando você configura a configuração de DPI alto do aplicativo Citrix Workspace para Sim, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.
- O Microsoft Teams 2.1 suporta o redirecionamento de apenas uma webcam por vez. No entanto, ele não suporta redirecionamento de várias webcams ou redirecionamento de webcam plug and play (PnP) em VDAs de sessão única.

### Limitação no aplicativo Citrix Workspace e no VDA

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente – não no VDA.

Para mais detalhes sobre as limitações da Microsoft, consulte Recursos não suportados em VDI.

# Nova solução VDI para Teams

**Observação:**

A Nova solução VDI para Teams está atualmente disponível para endpoints Windows e Mac no Citrix®. Esta solução requer uma versão mínima do Microsoft Teams. Consulte Requisitos do sistema.

Na Nova solução VDI para Teams, a Microsoft usa o SDK do Citrix Virtual Channel para construir canais virtuais personalizados. No endpoint, a mídia é descarregada para o mecanismo de mídia da Microsoft (SlimCore) em vez de `HdxRtcEngine`. Os canais virtuais personalizados transportam a comunicação entre o Teams no VDA e o mecanismo de mídia no endpoint.

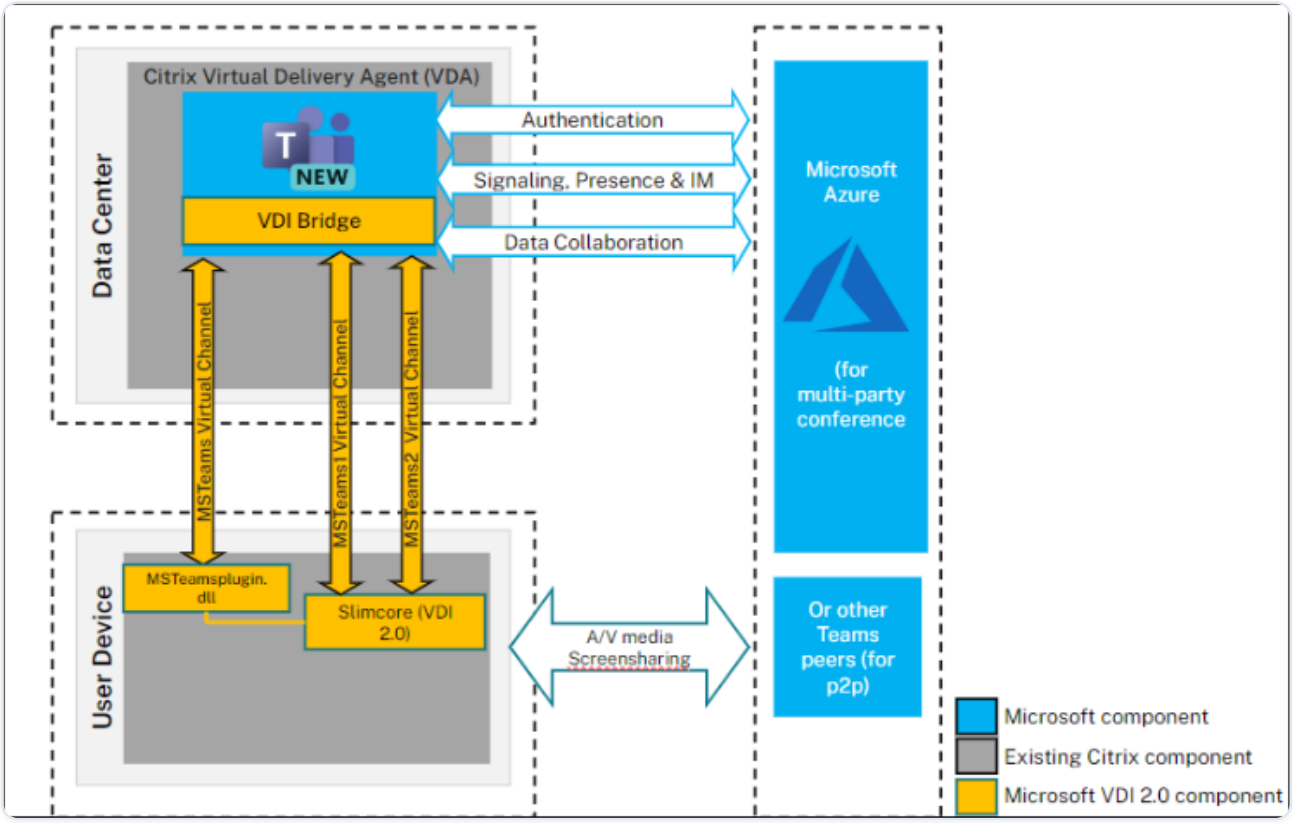
**Observação:**

A Microsoft anunciou a descontinuação da otimização Citrix HDX™ baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

- October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.
- April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

Recomenda-se que os clientes migrem para a Nova solução VDI para Teams. Esta alteração afeta apenas os endpoints Windows. Os endpoints macOS, Linux, ChromeOS e HTML5 não são impactados. Para mais detalhes, consulte Blog da Microsoft.

Esta solução é de propriedade e gerenciada pela Microsoft. A Citrix oferece suporte aos componentes Citrix envolvidos: aplicativo Citrix Workspace™, a lista de permissões de canais virtuais e os mecanismos de implantação de plug-ins descritos nesta página. Para a arquitetura de propriedade da Microsoft e detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.




## Requisitos do sistema

Esta seção lista as versões mínimas e recomendadas necessárias para suportar a Nova solução VDI para Teams. Em versões mínimas, algumas correções de bugs críticas ou os recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para a melhor experiência.

### Virtual Delivery Agent (VDA)

**Observação:**

Se você estiver usando 2203 LTSR CU2 ou inferior, ou 2303 CR ou inferior, consulte CTX682593 para entender as limitações nessas versões e planejar sua atualização.

| VERSÕES MÍNIMAS | VERSÕES RECOMENDADAS |
|---|---|
| 2203 LTSR CU3; 2305 CR | 2203 LTSR CU5+; 2402 LTSR e qualquer CR posterior |

### Aplicativo Citrix Workspace para Windows

| VERSÕES MÍNIMAS | VERSÕES RECOMENDADAS |
|---|---|
| 2203 LTSR (CU mais recente); 2302 CR | 2402 LTSR; 2405 CR ou posterior |

### Aplicativo Citrix Workspace para Mac

| VERSÕES MÍNIMAS | VERSÕES RECOMENDADAS |
|---|---|
| 2508.10 | 2607 ou posterior |

Os endpoints Mac exigem macOS 14, 15 ou 26. O macOS 26 exige o aplicativo Citrix Workspace 2511 ou posterior. No aplicativo Citrix Workspace para Mac 2508.10, o plug-in deve ser instalado manualmente. A opção de instalar o plug-in através do aplicativo Citrix Workspace, do Gerenciamento de Aplicativos Cliente ou do gerenciador de plug-ins de canal virtual está disponível a partir do aplicativo Citrix Workspace para Mac 2603.

Para a versão mínima do Microsoft Teams, requisitos de SO do endpoint e requisitos de hardware, consulte a documentação Microsoft.

## Componentes

- Novo Teams `vdiBridge`: o módulo de canal virtual do lado do servidor, empacotado com o Teams.
- Canal virtual personalizado (VC): o VC personalizado de propriedade do Microsoft Teams.
- Plug-in: a DLL do VC do lado do cliente. Responsável pelo download e limpeza do mecanismo de mídia.
- Mecanismo de mídia (SlimCore): o mecanismo de mídia específico do sistema operacional, entregue pela Microsoft como um pacote MSIX.

## Implantação

1. Certifique-se de ter a versão do Microsoft Teams listada em Pré-requisitos.
2. Configure a política **Lista de permissões de canais virtuais** para permitir os canais virtuais do Microsoft Teams. Esses canais permitem que o cliente Teams se conecte ao plug-in do lado do cliente. Para obter mais informações, consulte Segurança do canal virtual.

   A solução precisa de três canais virtuais personalizados. Use curingas para permitir o executável `ms-teams.exe` e os canais virtuais personalizados:

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

**Observação:**

- O VDA 2603 e posterior permitem esses três canais virtuais por padrão. Nenhuma configuração de política do Studio é necessária nessas versões.
- Os curingas para a política de lista de permissões de canais virtuais estão disponíveis no CVAD 2203 LTSR CU2 e posterior, ou no Citrix Virtual Apps and Desktops™ 2206 CR e posterior.
- As máquinas VDA devem ser reiniciadas para que a política entre em vigor.
- O caminho de instalação do MSTeams muda porque é um aplicativo MSIX, portanto, são necessários curingas. Permita as linhas exatas mostradas acima.

3. Esta solução é controlada por uma política do lado do Microsoft Teams, não por uma política da Citrix. Ela é habilitada por padrão. Para habilitá-la ou desabilitá-la para grupos de usuários específicos, consulte a documentação da Microsoft.
4. Implante o plug-in do Teams em seus endpoints. Consulte Opções para instalar o plug-in do Teams.
5. Para o estágio e registro do mecanismo de mídia, e as políticas de grupo que podem bloquear a instalação do MSIX, consulte a documentação da Microsoft.

### Opções para instalar o plug-in do Teams

Independentemente do método de instalação, o plug-in é colocado no local do aplicativo Citrix Workspace no endpoint:

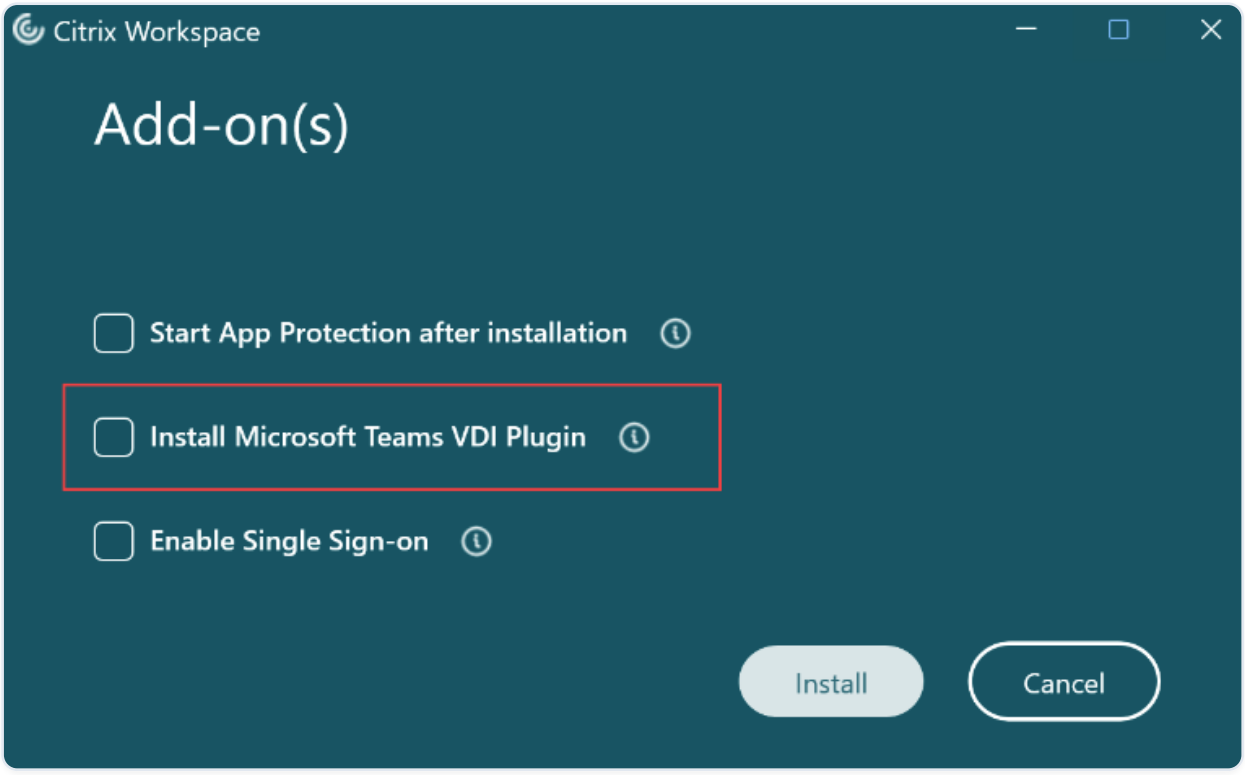
- Windows (`MsTeamsPluginCitrix.dll`): 64 bits `C:\Program Files (x86)\Citrix\ICA Client`; 32 bits `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

**Observação:**

- No Windows, instale o aplicativo Citrix Workspace no modo de administrador para que os canais virtuais sejam abertos corretamente. A instalação por usuário do aplicativo Citrix Workspace não é suportada.
- O plug-in VDI do Microsoft Teams não é suportado quando o aplicativo Citrix Workspace é instalado da Microsoft Store.
- A instalação do plug-in para se nenhum aplicativo Citrix Workspace for encontrado no endpoint.
- No Windows, o plug-in e o aplicativo Citrix Workspace devem ter a mesma arquitetura. Um aplicativo Citrix Workspace de 32 bits não pode carregar um plug-in de 64 bits.
- Os plug-ins podem ser atualizados ou reparados, mas não podem ser revertidos para uma versão anterior, e somente enquanto não houver uma sessão ativa.

### Opção 1: Através da instalação do aplicativo Citrix Workspace

- **Windows:** Durante uma nova instalação ou atualização manual, selecione **Install Microsoft Teams VDI Plugin** na página **Add-on(s)**. A partir do aplicativo Citrix Workspace para Windows 2508, esta opção é selecionada por padrão. Desmarque-a para pular a instalação. As atualizações lembram sua seleção anterior.



Você também pode instalar pela linha de comando com o switch `/InstallMSTeamsPlugin`. Por exemplo, `CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` instala o plug-in, e `/InstallMSTeamsPlugin=N` o impede.

Para uma nova instalação, o mínimo é o aplicativo Citrix Workspace para Windows 2402 LTSR. Para atualizações no local, o mínimo é o aplicativo Citrix Workspace para Windows 2405 CR. Para os detalhes mais recentes, consulte Instalar plug-ins de terceiros.

- **Mac:** A opção de instalar o plug-in durante a instalação do aplicativo Citrix Workspace está disponível a partir do aplicativo Citrix Workspace para Mac 2603 e requer ação do usuário. O aplicativo Citrix Workspace para Mac 2607 instala o plug-in automaticamente por padrão. No aplicativo Citrix Workspace para Mac 2508.10, instale o plug-in manualmente. Consulte Opção 2: Baixar o plug-in diretamente.

**Opção 2: Baixar o plug-in diretamente**

- **Windows:** Baixe o MSI e implante-o com ferramentas como SCCM ou Intune sobre qualquer versão suportada do aplicativo Citrix Workspace:
  - Aplicativo Citrix Workspace de 32 bits: aka.ms/plugin
  - Aplicativo Citrix Workspace de 64 bits: aka.ms/plugin_x64
  - Aplicativo Citrix Workspace baseado em Arm: aka.ms/plugin_arm64
- **Mac:** Baixe o plug-in em aka.ms/macplugin e implante-o com ferramentas como JAMF.

**Opção 3: Gerenciamento de Aplicativos Cliente (anteriormente serviço Global App Configuration)**

O Gerenciamento de Aplicativos Cliente (anteriormente serviço Global App Configuration, ou GACS) gerencia as configurações de aplicativos para endpoints gerenciados e não gerenciados, e pode implantar o plug-in do Teams em seus endpoints. No Mac, isso requer o aplicativo Citrix Workspace para Mac 2603 ou posterior. Consulte Gerenciamento de plug-in VDI do Microsoft Teams.

**Opção 4: Gerenciador de plug-in de canal virtual**

O gerenciador de plug-in de canal virtual implanta plug-ins em endpoints de cliente para aplicativos que precisam de componentes de endpoint, incluindo a nova solução VDI para Teams. Ele detecta o aplicativo em execução no VDA e solicita ao usuário que instale o plug-in no endpoint. Os administradores podem usá-lo em cenários BYOD. No Mac, isso requer o aplicativo Citrix Workspace para Mac 2603 ou posterior. Consulte Gerenciador de plug-in de canal virtual.

### Cenários de atualização de plug-in

A Citrix gerencia as atualizações do plug-in do Teams de forma transparente quando o plug-in é instalado através das Opções 1, 3 ou 4. Se o plug-in for instalado manualmente (Opção 2), a Citrix não manipular as atualizações.

- Certifique-se de que a atualização automática do aplicativo Citrix Workspace esteja ativada para atualizações automáticas de plug-in.
- Garanta um mínimo do aplicativo Citrix Workspace para Windows 2405. O aplicativo Citrix Workspace para Windows 2508 ou posterior instala o plug-in automaticamente quando o aplicativo Citrix Workspace é atualizado automaticamente.
- A Citrix não manipular a desinstalação do plug-in. Desinstale o plug-in separadamente quando necessário.

> **Observação:**
>
> A Citrix gerencia as atualizações do plug-in do Teams, não do mecanismo de mídia. A Microsoft entrega e atualiza o mecanismo de mídia.

### Teams como um aplicativo publicado da Citrix

O Teams publicado como um aplicativo Citrix Virtual Apps pode ser otimizado com esta solução quando todos os componentes necessários atenderem às versões mínimas. Para as versões necessárias e limitações conhecidas, consulte a documentação da Microsoft.

### Interoperabilidade e roaming

Consulte Otimização para Microsoft Teams para saber como a nova solução VDI para Teams e a Otimização Citrix HDX interoperam e como o roaming se comporta.

### Considerações de rede

Consulte Considerações de rede na documentação da Microsoft.

### Suporte a recursos

O conjunto de recursos e a implementação são de propriedade da Microsoft. Consulte a lista de recursos na documentação da Microsoft.

### Solução de problemas

O cliente Microsoft Teams relata o status de otimização e, quando a otimização falha, um código de erro. Esses indicadores de status e códigos de erro são definidos pela Microsoft. Para a lista completa e solução de problemas de ponta a ponta, consulte Solução de problemas da nova solução VDI para Teams na documentação da Microsoft.

O Citrix Monitor oferece visibilidade do estado de otimização dessa solução. Nos detalhes de uma sessão, a exibição Topologia da Sessão mostra se o aplicativo está otimizado e sinaliza quaisquer componentes ausentes, como o gerenciador de plug-ins, o plug-in e sua versão, o estado do canal virtual e o status da lista de permissões do canal virtual. Para obter mais informações, consulte Visibilidade da otimização de comunicações em tempo real.

Alguns códigos de erro da Microsoft apontam para a configuração do lado da Citrix. Verificações comuns da Citrix:

- Se o cliente Teams relatar que os canais virtuais personalizados estão bloqueados (erro da Microsoft 2003), confirme se a lista de permissões de canais virtuais inclui MSTEAMS, MSTEAM1 e MSTEAM2.
- Se o cliente Teams relatar que nenhum plug-in foi detectado (erro da Microsoft 2000), confirme se o plug-in está instalado e carregado. No Process Explorer, selecione `wfica32.exe`, mostre o painel inferior e verifique a guia DLL para `MsTeamsPluginCitrix.dll`.
- Se o cliente Teams relatar uma versão não suportada do Citrix Workspace app (erro da Microsoft 2004), atualize para uma versão suportada. Consulte Requisitos do sistema.

### Limitações conhecidas

Os recursos e a implementação são de propriedade da Microsoft. Consulte Problemas conhecidos na documentação da Microsoft.

# Otimização para Microsoft Teams (Clássico)

> **Nota:**
>
> O novo Microsoft Teams 2.1 já está geralmente disponível para VDA. Esta versão do Microsoft Teams é compatível com a Otimização do Citrix Microsoft Teams usando WebRTC. Para obter mais informações sobre a Otimização para o Novo Teams, consulte MS Teams New

> A partir do Citrix Virtual Apps and Desktops 2402, você não precisa configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela é permitida por padrão.

> Os aplicativos publicados agora são compatíveis com o novo Microsoft Teams.

> A Citrix oferece otimização para Microsoft Teams baseado em desktop usando Citrix Virtual Apps and Desktops™ e o aplicativo Citrix Workspace™. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

Nossa otimização para Microsoft Teams inclui serviços HDX™ do lado do VDA e uma API para interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O endpoint decodifica e fornece o multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem nativamente no aplicativo hospedado do Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um canal virtual de comando e controle. Isso significa que a mídia não é trocada entre o aplicativo Citrix Workspace e o VDA.

Apenas client-fetch/client-render está disponível.

Esta demonstração em vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



## Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam a versão mais recente disponível do Microsoft Teams e que ela seja mantida atualizada. As versões do aplicativo de desktop do Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas. As versões não suportadas do aplicativo de desktop do Microsoft Teams exibem uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Microsoft Teams (Desktop e Mac).

Recomendamos que você siga as diretrizes de instalação em toda a máquina do Microsoft Teams. Evite usar o instalador .exe que instala o Microsoft Teams em `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` da linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Ao definir este parâmetro, o Instalador do Microsoft Teams para toda a máquina aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem então desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro `ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` apenas em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não se atualiza automaticamente sempre que há uma nova versão. Recomendamos este modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou desktops de um Windows Server ou catálogos aleatórios/agrupados do Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação VDI).

Suponha que você tenha um ambiente VDI persistente dedicado do Windows 10. Você deseja que o aplicativo Microsoft Teams seja atualizado automaticamente e prefere que o Microsoft Teams seja instalado por usuário em `Appdata/Local`. Nesse caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> A Citrix recomenda instalar o VDA antes de instalar o Microsoft Teams na imagem dourada. Essa ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA, desinstale e reinstale o Microsoft Teams.

## Para Acesso Remoto a PC

A Citrix recomenda que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior após a instalação do VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 e posteriores incluem lógica aumentada executada no momento do lançamento do Microsoft Teams e no momento do login para detecção do VDA. Essas versões também incluem identificação do tipo de sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem falhar ao detectar e desabilitar certos recursos ou elementos da interface do usuário. Por exemplo, Salas de Apoio, janelas pop-out para reuniões e bate-papos, ou reações de reunião.

> **Importante:**
>
> Quando você alterna de uma sessão local para uma sessão HDX e se o Microsoft Teams for mantido aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar corretamente com o HDX. Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Ao trabalhar no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do Acesso Remoto ao PC (HDX ou local). Isso ocorre porque o Microsoft Teams só pode avaliar o modo VDI no momento do lançamento do aplicativo, e não enquanto já está em execução em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-out, Salas de Apoio ou reações de reunião.

## Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, você deve criar uma chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` na linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em Multimídia.

## Recomendações de Gerenciamento de Perfil

Recomendamos usar o instalador para toda a máquina para ambientes Windows Server e VDI agrupado do Windows 10.

Quando o sinalizador **ALLUSER=1** é passado para o MSI a partir da linha de comando (o instalador para toda a máquina), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**

> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> Um logon de usuário subsequente aciona a instalação final em **AppData**.

### Instalador para toda a máquina

A seguir, um exemplo de pastas, atalhos da área de trabalho e registros criados pela instalação de um instalador do Microsoft Teams para toda a máquina em uma VM do Windows Server 2016 de 64 bits:

*Pasta:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Atalho da Área de Trabalho:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Registro:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`

- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> O local do registro varia de acordo com os sistemas operacionais subjacentes e a arquitetura.

### Recomendações

- Recomendamos desativar a inicialização automática excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do seu dia de trabalho) aumentem o uso da CPU da VM.
- Se a área de trabalho virtual não tiver uma GPU/vGPU, recomendamos definir **Desabilitar aceleração de hardware da GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada em `%Appdata%\Microsoft\Teams` em `desktop-config.json`. Você pode usar um script de logon para editar esse arquivo e definir o valor como `true`.
- Se estiver usando o Citrix Workspace Environment Management™ (WEM), ative a **Proteção contra Picos de CPU** para gerenciar o consumo do processador para o Microsoft Teams.

### Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação difere. Todos os arquivos são colocados em AppData.

*Pasta:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Atalho na área de trabalho:*

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

*Registro:*

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

## Práticas recomendadas

As recomendações de melhores práticas são baseadas nos cenários de caso de uso. Usar o Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para 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 nestas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

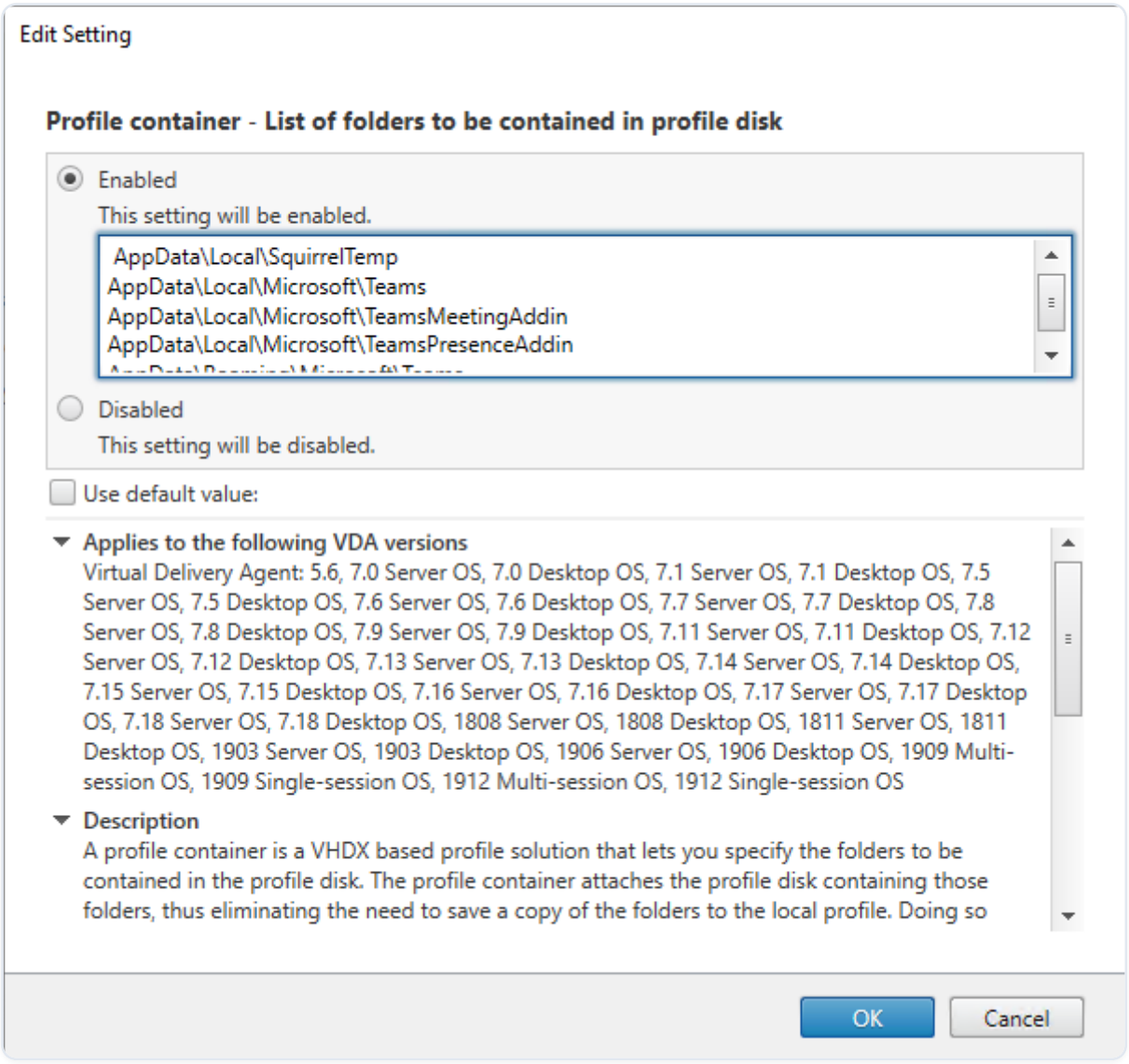
### Lista de exclusão de conteúdo em cache do Microsoft Teams para configuração não persistente

Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams conforme descrito na documentação Microsoft. Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais sua configuração não persistente.

### Caso de uso: cenário de sessão única

Nesse cenário, o usuário final usa o Microsoft Teams em um local por vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop, e o Microsoft Teams é implantado no desktop virtual como um aplicativo. Recomendamos habilitar o contêiner de perfil do Citrix e redirecionar os diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador do Microsoft Teams para toda a máquina (**ALLUSER=1**) na imagem dourada.
2. Habilite o Citrix Profile Management e configure o armazenamento de perfil de usuário com as permissões adequadas.
3. Habilite a seguinte configuração de política do Profile Management: **Sistema de arquivos > Sincronização > Contêiner de perfil – Lista de pastas a serem contidas no disco de perfil**.




Liste todos os diretórios por usuário nesta configuração. Você também pode configurar essas definições usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

## Requisitos do sistema

### Versão mínima recomendada - Delivery Controller (DDCs) 1906.2

Se você estiver usando uma versão anterior, consulte Habilitar otimização do Microsoft Teams:

Sistemas operacionais suportados:

- Windows Server 2022, 2019, 2016, 2012R2 Standard e edições de data center, e com a opção Server Core

### Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais suportados:

- Windows 11
- Windows 10 64 bits, versões 1607 e posteriores. Aplicativos hospedados em VM são suportados no aplicativo Citrix Workspace para Windows 2109.1 e posterior
- Windows Server 2022, 2019, 2016 e 2012 R2 (Edições Standard e Datacenter)

Requisitos:

- BCR_x64.msi - o MSI que inclui o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não o exclua.

### Versão recomendada – Citrix Workspace app para Windows CR mais recente e Versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 e 64 bits, incluindo edições Embedded) (O suporte para Windows 7 foi interrompido na Versão 2006) (O suporte para Windows 8.1 foi interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas de processador (CPU) suportadas: x86 e x64 (ARM não é suportado).
- Requisito de endpoint: CPU dual-core de aproximadamente 2,2–2,4 GHz que pode suportar resolução HD de 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs dual ou quad-core com velocidades base mais baixas (~1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Thin Clients HP verificados: t630/t640, t730/t740, mt44/mt45.
- Thin Clients Dell verificados: 5070, 5470 Mobile TC e AIO.
- Thin Clients 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de endpoints verificados, consulte Thin Clients.
- O aplicativo Citrix Workspace requer pelo menos 600 MB de espaço livre em disco e 1 GB de RAM.
- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se ele não estiver presente no sistema.

Os administradores podem habilitar/desabilitar o Microsoft Teams iniciando no modo otimizado, alterando a política de otimização do Microsoft Teams. Os usuários que iniciam no modo otimizado no aplicativo Citrix Workspace não podem desabilitar o Microsoft Teams.

### Versão mínima - aplicativo Citrix Workspace 2006 para Linux

Para obter mais informações, consulte Otimização para Microsoft Teams na documentação do aplicativo Citrix Workspace para Linux.

Software:

- `GStreamer` 1.0 ou posterior ou Cairo 2
- `libc++-9.0` ou posterior
- `libgdk` 3.22 ou posterior
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 ou posterior

Aprimoramento de autenticação:

- Biblioteca Libsecret
- Biblioteca libunwind-12. Para obter mais informações, consulte Adicionando a dependência da biblioteca libunwind-12 para llvm-12.

Hardware:

- CPU dual-core de no mínimo 1,8 GHz que suporte resolução HD de 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com velocidade base de 1,8 GHz e alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de endpoints verificados, consulte Thin Clients.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desabilitar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é VDWEBRTC=On. Após a conclusão da atualização, reinicie a Sessão. (É necessária permissão de root).

### Versão mínima - aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais suportados:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e posterior.
- macOS Monterey.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Observação:**

> O aplicativo Citrix Viewer requer acesso às preferências de Segurança e Privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência em **Menu Apple > Preferências do Sistema > Segurança e Privacidade > Guia Privacidade > Gravação de tela** e selecionam **Citrix Viewer**.

> A otimização do Microsoft Teams funciona por padrão com o aplicativo Citrix Workspace 2012 e posterior e macOS 10.15.

Se você deseja desabilitar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

### Versão mínima - Versão mais recente do aplicativo Citrix Workspace para ChromeOS executando a versão mais recente do ChromeOS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core 2.4 GHz.

Recursos suportados:

- Áudio
- Vídeo

- Otimização de compartilhamento de tela (entrada e saída) - desabilitada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

## Escalabilidade de Servidor Único

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) podem ser suportados em um único host físico. Isso é comumente referido como Escalabilidade de Servidor Único (SSS) do Citrix Virtual Apps and Desktops. No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade de usuário. A ideia é descobrir quantos usuários ou VMs podem ser executados em uma única peça de hardware executando um hypervisor principal.

> **Nota:**
>
> Esta seção inclui orientações para estimar o SSS. As orientações são de alto nível e podem não ser necessariamente específicas para sua situação ou ambiente exclusivo. A única maneira de realmente entender o SSS do Citrix Virtual Apps and Desktops é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda usar estas orientações e estas regras simples apenas para estimar rapidamente o SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de adquirir hardware ou tomar qualquer decisão financeira.

### Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2,60 GHz (Turbo máximo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- Armazenamento SSD local RAID 0 (11 discos) 6 TB

### Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

### Terminologia

- Carga de trabalho de trabalhador do conhecimento: Inclui Acrobat Reader, Freemind/Java, Visualizador de fotos, Edge e aplicativos do MS Office, como Excel, Outlook, PowerPoint e Word.
- Linha de base: Testes de escalabilidade de servidor executados com carga de trabalho de trabalhador do conhecimento (sem Microsoft Teams).
- Carga de trabalho do Microsoft Teams: Carga de trabalho típica de trabalhador do conhecimento + Microsoft Teams.

### Como o Microsoft Teams é testado sob estresse

- O Microsoft Teams é otimizado com HDX. Assim, todo o processamento multimídia é descarregado para o endpoint ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou encerrados antes do início da carga de trabalho.
- Abrir o Microsoft Teams (Inicialização a frio).
- Medir o tempo que o Microsoft Teams leva para carregar e focar na janela principal do Microsoft Teams.
- Alternar para a janela de chat usando atalhos de teclado.
- Alternar para a janela do calendário usando atalhos de teclado.
- Enviar a mensagem de chat para um usuário específico usando atalhos de teclado.
- Alternar para a janela do Microsoft Teams usando atalhos de teclado.

### Resultados

- Impacto de 40% na escalabilidade com a Carga de Trabalho do Microsoft Teams (81 usuários), em comparação com a Linha de Base (137 usuários).
- Aumentar a capacidade do servidor em ~40% (em CPU) restaura o número de usuários como na carga de trabalho de Linha de Base.
- 20% de memória extra necessária com a Carga de Trabalho do Microsoft Teams, em comparação com a Linha de Base.
- Aumentar o tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% na gravação de IOPS, aumento de ~100% na leitura de IOPS. O Microsoft Teams pode ter um impacto significativo em um ambiente com armazenamento mais lento.

# Matriz de recursos e suporte de versão

| RECURSO | MICROSOFT TEAMS (VERSÃO MÍNIMA) | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA MAC (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA LINUX (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA CHROME OS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|---|
| Áudio/Vídeo (P2P e conferência) | versão atual menos 90 dias | 1906 | 1907 | 2009 | 2004 | 2105.5 |
| Compartilhamento de tela | Versão atual menos 90 dias | 1906 | 1907 | 2012 | 2006 | 2105.5 |
| i. Borda vermelha do indicador de tela | Versão atual menos 90 dias | 1906 | 2002 | 2012 | 2006 | Não |
| ii. Limitar a captura ao Desktop Viewer | Versão atual menos 90 dias | 1906 | 2009.5 | 2012 | 2006 | Não |
| iii. Vários monitores | Versão atual menos 90 dias | 1912 CU6+ | 2106 (1) | 2106 | 2106 | Não |
| DTMF | Versão atual | N/A | 2102 | 2101 | 2101 | 2111.1 |

| RECURSO | MICROSOFT TEAMS (VERSÃO MÍNIMA) | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA MAC (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA LINUX (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA CHROME OS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|---|
| | menos 90 dias | | | | | |
| Suporte a Servidor Proxy | Versão atual menos 90 dias | N/A | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| Compartilhamento de apps | Versão atual menos 90 dias | 2109 | 2109.1 | 2203.1 | 2209 | Não |
| Legendas ao Vivo | Versão atual menos 90 dias | N/A (4) | 2109.1 | 2109 | 2109 | 2303 |
| e911 Dinâmico | Versão atual menos 90 dias | N/A | 2112.1 | 2112 | 2112 | 2112 |
| Conceder Controle | Versão atual menos 90 dias | N/A | 2112.1 | 2203.1 | Não | Não |
| Solicitar Controle | Versão atual menos 90 dias | N/A | 2112.1 | 2203.1 | 2203 | 2303 |

| RECURSO | MICROSOFT TEAMS (VERSÃO MÍNIMA) | VDA (VERSÃO MÍNIMA) | CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA MAC (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA LINUX (VERSÃO MÍNIMA) | APLICATIVO CITRIX WORKSPACE PARA CHROME OS (VERSÃO MÍNIMA) |
|---|---|---|---|---|---|---|
| MultiWindow | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Transcrições de Reunião | Versão atual menos 90 dias | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Desfoque de Plano de Fundo | Versão atual menos 90 dias | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. CD Viewer apenas em modo de tela cheia. SHIFT+F2 não é suportado.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, as Legendas ao Vivo (Live Captions) só funcionarão 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 forma diferente se o Microsoft Teams estiver no modo de UI de Janela Única (Single Window UI) ou no modo MultiJanela (MultiWindow).
5. O MultiWindow foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

**Nota:**

- Todos os recursos listados em **Citrix Workspace app para Windows 1912 CU6 (ou posterior)** são aplicáveis ao Citrix Workspace app para Windows 2203.1 LTSR CU1.
- A Microsoft descontinuou o suporte para o modo de Janela Única no Microsoft Teams. Para cumprir, você deve atualizar seu VDA para 1912 CU6+ LTSR e o aplicativo Citrix Workspace 2203 CU2+ ou superior, que suporta o modo MultiWindow.

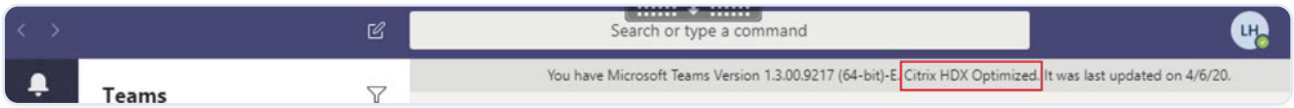
## Habilitar otimização do Microsoft Teams

Para habilitar a otimização para o Microsoft Teams, use a política do console de gerenciamento descrita na política (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/multimedia-policy-settings.html#microsoft-teams-redirection). Esta política está **ATIVADA** por padrão. Além de esta política estar habilitada, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima exigida. Se você habilitou a política e a versão do aplicativo Citrix Workspace é suportada, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definido como **1** automaticamente no VDA. O Microsoft Teams lê a chave para carregar no modo VDI.

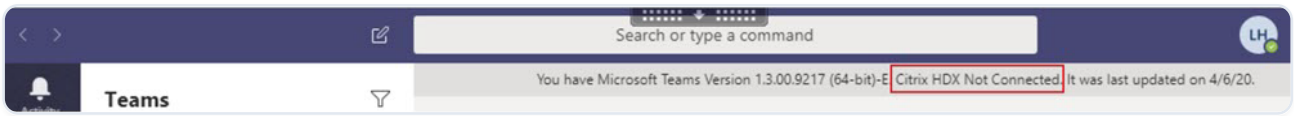
**Nota:**

Se você estiver usando VDAs versão 1906.2 ou posterior ou com versões de controlador mais antigas (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda pode ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

Se você clicar em **Sobre > Versão**, a legenda **Citrix HDX Optimized** será exibida:

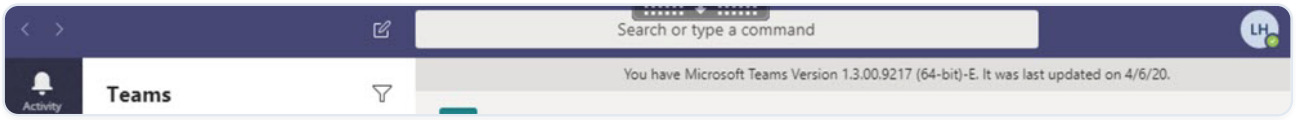



Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro nas partes posteriores da pilha. O erro provavelmente está nos serviços VDA ou no aplicativo Citrix Workspace.




Se você não vir nenhuma legenda, o Microsoft Teams falhou ao carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito do mouse no ícone da área de notificação e

reiniciando. Certifique-se de que a política do console de gerenciamento não esteja definida como **Proibida** e que a versão do aplicativo Citrix Workspace seja suportada.




**Importante: reconexões de sessão**

- Pode ser necessário reiniciar o Microsoft Teams para obter uma sessão otimizada por HDX quando sua conectividade mudar. Por exemplo, se você estiver migrando de um endpoint não compatível (aplicativo Workspace para iOS, Android ou versões antigas de Windows/Linux/Mac) para um compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou vice-versa.
- Uma reinicialização do Microsoft Teams também é necessária se você instalou o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações VDI persistentes. Nesses casos, o Microsoft Teams pode ser atualizado automaticamente enquanto a sessão HDX está no estado desconectado. Assim, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado de forma otimizada.
- Ao migrar de uma sessão local para uma sessão HDX, você deve reiniciar o Microsoft Teams para otimizar com HDX. Esta ação é necessária em um cenário de Acesso Remoto a PC.

## Requisitos de rede

O Microsoft Teams depende de servidores Media Processor no Microsoft 365 para reuniões ou chamadas multipartidárias. Além disso, o Microsoft Teams depende dos Microsoft 365 Transport Relays para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Assim, a saúde da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Consulte Princípios de conectividade de rede do Microsoft 365 para obter diretrizes detalhadas sobre o planejamento de rede.

Recomendamos avaliar seu ambiente para identificar quaisquer riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem. Use a Ferramenta de Avaliação de Rede do Skype for Business para testar se sua rede está pronta para o Microsoft Teams. Para obter informações de suporte, consulte Suporte.

### Resumo das principais recomendações de rede para tráfego do Protocolo de Tempo Real (RTP)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir do escritório da filial.
- Planeje e forneça largura de banda suficiente no escritório da filial.
- Verifique a conectividade e a qualidade da rede em cada escritório da filial.
- Se você precisar usar qualquer um dos seguintes na filial, certifique-se de que o tráfego RTP/UDP (tratado por HdxRtcEngine.exe no aplicativo Citrix Workspace) não seja impedido.
    - Ignorar servidores proxy
    - Interceptação de SSL de rede
    - Dispositivos de inspeção profunda de pacotes
    - Hairpins de VPN (use tunelamento dividido, se possível)

**Importante: Configuração de tunelamento dividido de VPN**

O tráfego de HdxRtcEngine.exe deve ser desviado do túnel VPN e permitido usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira como isso é realizado depende do produto VPN e da plataforma da máquina utilizada, mas a maioria das soluções VPN permite alguma configuração simples de política para aplicar essa lógica. Para obter mais informações sobre a orientação de túnel dividido específica da plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o Protocolo de Transporte Seguro em Tempo Real (SRTP) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para este recurso, chaves simétricas (negociadas com DTLS) são usadas para criptografar mídia e mensagens de controle usando a cifra de criptografia AES.

As seguintes métricas são recomendadas para uma experiência de usuário positiva:

| MÉTRICA | PONTO DE EXTREMIDADE PARA MICROSOFT 365 |
|---|---|
| Latência (sentido único) | < 50 ms |
| Latência (RTT) | < 100 ms |
| Perda de Pacotes | <1% durante qualquer intervalo de 15s |
| Jitter de interchegada de pacotes | <30ms durante qualquer intervalo de 15s |

Para obter mais informações, consulte Prepare a rede da sua organização para o Microsoft Teams.

Para requisitos de largura de banda, a otimização para Microsoft Teams pode usar uma ampla variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam esses codecs durante o processo de estabelecimento da chamada usando o Protocolo de Descrição de Sessão (SDP) Oferta/Resposta. As recomendações mínimas da Citrix por usuário são:

| TIPO | LARGURA DE BANDA | CODEC |
|---|---|---|
| Áudio (em cada sentido) | Cerca de 90 kbps | G.722 |
| Áudio (em cada sentido) | Cerca de 60 kbps | Opus* |
| Vídeo (em cada sentido) | Aproximadamente 700 kbps | H264 360p a 30 quadros por segundo 16:9 |
| Compartilhamento de tela | Aproximadamente 300 kbps | H264 1080p a 15 quadros por segundo |

* Opus suporta codificação de taxa de bits constante e variável de 6 kbps até 510 kbps.

Opus e H264 são os codecs preferenciais para chamadas ponto a ponto e de conferência.

> **Importante:**

> Sobre desempenho, a codificação é mais cara que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix

> Workspace para Linux e Windows. Consulte Estimador de desempenho do codificador e Otimização para Microsoft Teams.

## Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

  Se você configurar um servidor proxy explícito no VDA e rotear as conexões para localhost através de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Ignorar servidores proxy para endereços locais** em **Opções da Internet > Conexões > Configurações de LAN > Servidores Proxy** e ignorar `127.0.0.1:9002`.

  Se você usar um arquivo PAC, seu script de configuração de proxy do VDA do arquivo PAC deve retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

  Se a filial estiver configurada para acessar a internet através de um proxy, estas versões suportam servidores proxy:

  - Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
  - Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler as configurações de proxy. Esses dispositivos enviam tráfego diretamente para os servidores TURN do Microsoft 365.

> **Importante:**

- Verifique se o dispositivo cliente pode se conectar ao servidor DNS para fazer resoluções DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor de retransmissão do Microsoft Teams:
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

Se as solicitações DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e as chamadas em conferência com o estabelecimento de mídia falharão.

- A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não do cliente).

## Estabelecimento de chamadas e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão direta de rede Secure Real-time Transport Protocol (SRTP) sobre User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia retorna para TCP/TLS 443.

O mecanismo de mídia HDX oferece suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal Using Relays around NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Esse suporte significa que o endpoint deve ser capaz de realizar resoluções DNS.

Considere um cenário em que não há um caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está participando de uma chamada ou reunião multipartidária. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP de sub-rede do Microsoft 365 e quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver

bloqueado). Para obter mais informações, consulte o diagrama de arquitetura em Configuração de chamada e URLs e intervalos de endereços IP do Office 365 ID 11.

| ID | CATEGORIA | ENDEREÇOS | PORTAS DE DESTINO |
|---|---|---|---|
| 11 | Otimização necessária | 13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (alternativa) |

Esses intervalos incluem tanto os Transport Relays quanto os processadores de mídia, com um Azure Load Balancer como front-end. Os Transport Relays do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são endpoints ICE. Além disso, os Transport Relays do Microsoft Teams não encerram mídia, TLS ou realizam qualquer transcodificação. Eles podem fazer a ponte de TCP (se HdxRtcEngine.exe usar TCP) para UDP ao encaminhar tráfego para outros pares ou processadores de mídia.

O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com o Transport Relay do Microsoft Teams mais próximo na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e as portas UDP 3478–3481 (portas UDP diferentes por carga de trabalho, embora a multiplexação possa ocorrer) ou TCP/TLS 443 para alternativas. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado em vez do TCP, aconselhamos que você projete suas redes para acomodar o tráfego UDP no escritório remoto.

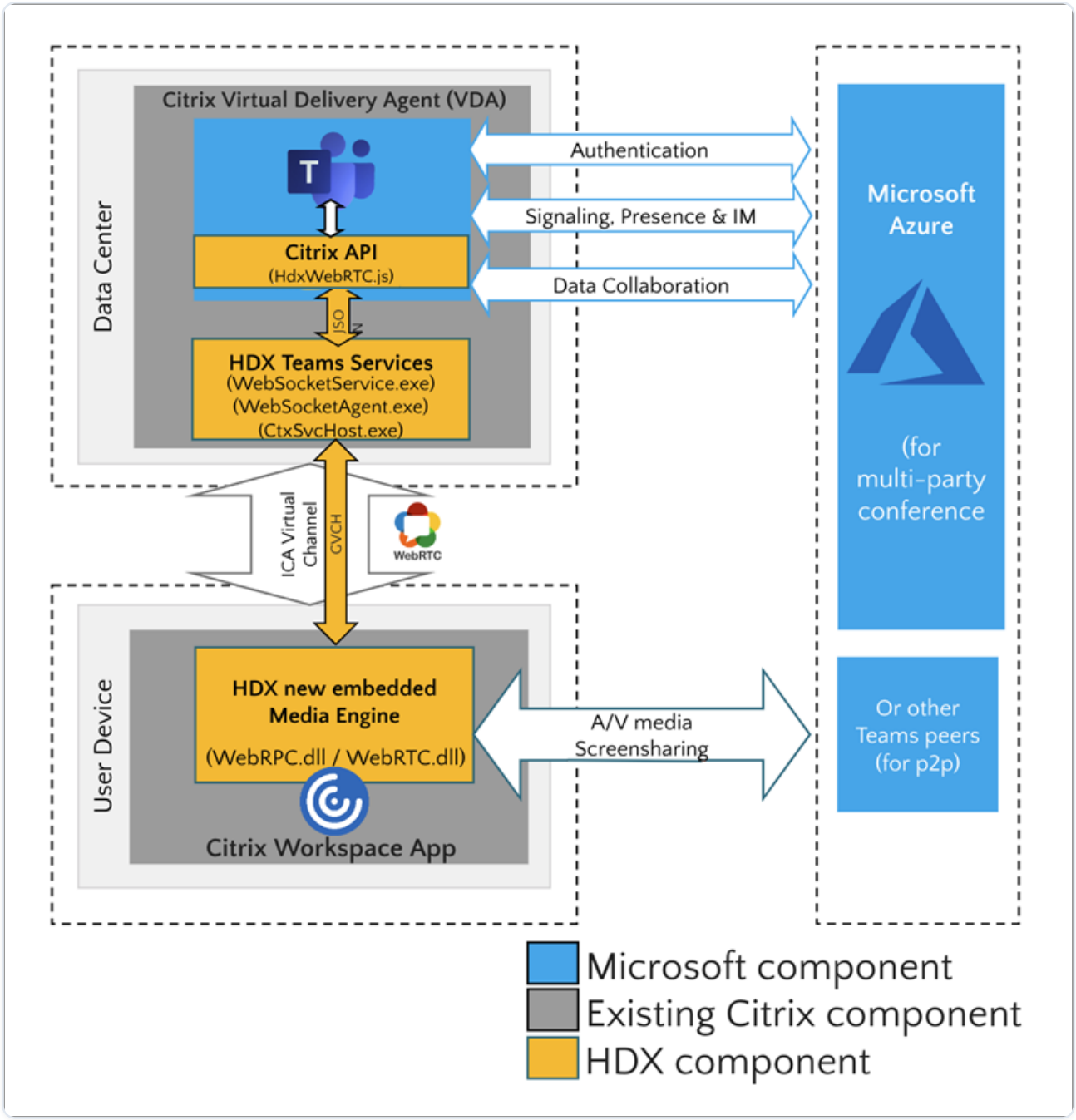
Se o Microsoft Teams for carregado no modo otimizado e HdxRtcEngine.exe estiver em execução no endpoint, falhas de ICE podem causar uma falha na configuração da chamada ou áudio/vídeo apenas unidirecional. Quando uma chamada não pode ser concluída ou os fluxos de mídia não são full duplex, verifique primeiro o **rastreamento do Wireshark** no endpoint. Para obter mais informações sobre o processo de coleta de candidatos ICE, consulte "Coleta de logs" na seção Suporte.

> **Nota:**
>
> Se os endpoints não tiverem acesso à internet, os usuários ainda poderão fazer uma chamada ponto a ponto se ambos estiverem na mesma LAN. As reuniões falham. Nesse caso, há um tempo limite de 30 segundos antes que a configuração da chamada comece.

### Configuração da chamada

Use este diagrama de arquitetura como referência visual para a sequência do fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.

#### Arquitetura




1. Iniciar o Microsoft Teams.
2. O Microsoft Teams autentica-se no O365. As políticas de locatário são enviadas para o cliente do Microsoft Teams, e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.

3. O Microsoft Teams detecta que está sendo executado em um VDA e faz chamadas de API para a API JavaScript da Citrix.
4. O JavaScript da Citrix no Microsoft Teams abre uma conexão WebSocket segura para o WebSocketService.exe em execução no VDA, que gera o WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico chamando o Serviço de Redirecionamento do Microsoft Teams HDX da Citrix (CtxSvcHost.exe).
6. O wfica32.exe (mecanismo HDX) do aplicativo Citrix Workspace gera um novo processo chamado HdxRtcEngine.exe, que é o novo mecanismo WebRTC usado para otimização do Microsoft Teams.
7. O mecanismo de mídia da Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem começar a processar solicitações multimídia.

   -----Chamadas do usuário------

8. **Par A** clica no botão **chamar**. O Teams.exe se comunica com os serviços do Microsoft Teams no Microsoft 365, estabelecendo um caminho de sinalização de ponta a ponta com o **Par B**. O Microsoft Teams solicita ao HdxRtcEngine uma série de parâmetros de chamada suportados (codecs, resoluções e assim por diante, o que é conhecido como uma oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são então retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e, de lá, para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização, e as verificações de conectividade ICE (travessia de NAT e Firewall usando solicitações de ligação STUN) são concluídas. Em seguida, a mídia Secure Real-time Transport Protocol (SRTP) flui diretamente entre HdxRtcEngine.exe e o outro par (ou servidores de conferência do Microsoft 365 se for uma reunião).

## Sistema Telefônico da Microsoft

O Phone System é a tecnologia da Microsoft que permite o controle de chamadas e PBX na nuvem do Microsoft 365 com o Microsoft Teams. A otimização para Microsoft Teams suporta o Phone System, usando Planos de Chamada do Microsoft 365 ou Roteamento Direto. Com o Roteamento Direto, você pode conectar seu próprio controlador de borda de sessão suportado diretamente ao Microsoft Phone System sem nenhum software local adicional. Filas de chamadas, transferência, encaminhamento, espera, mudo e retomada de uma chamada são suportados.

### DTMF

O recurso de multifrequência de tom duplo (DTMF) é suportado com estas versões do aplicativo Citrix Workspace (e posteriores):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para ChromeOS versão 2111.1

### Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado em Planos de Chamada da Microsoft, Operator Connect e Roteamento Direto, ele permite que você faça o seguinte:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace que é executado no endpoint, em vez do cliente Microsoft Teams que é executado no VDA.

A lei de Ray Baum exige que a localização despachável do chamador do 911 seja transmitida ao Ponto de Atendimento de Segurança Pública (PSAP) apropriado. A otimização do Microsoft Teams com HDX está em conformidade com a lei de Ray Baum quando usada com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Linux versão 2112 e posterior
- Aplicativo Citrix Workspace para Mac versão 2112 e posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2112 e posterior

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de rede ou de localização de emergência:

- Configurações de rede
- Serviço de Informações de Localização (LIS)

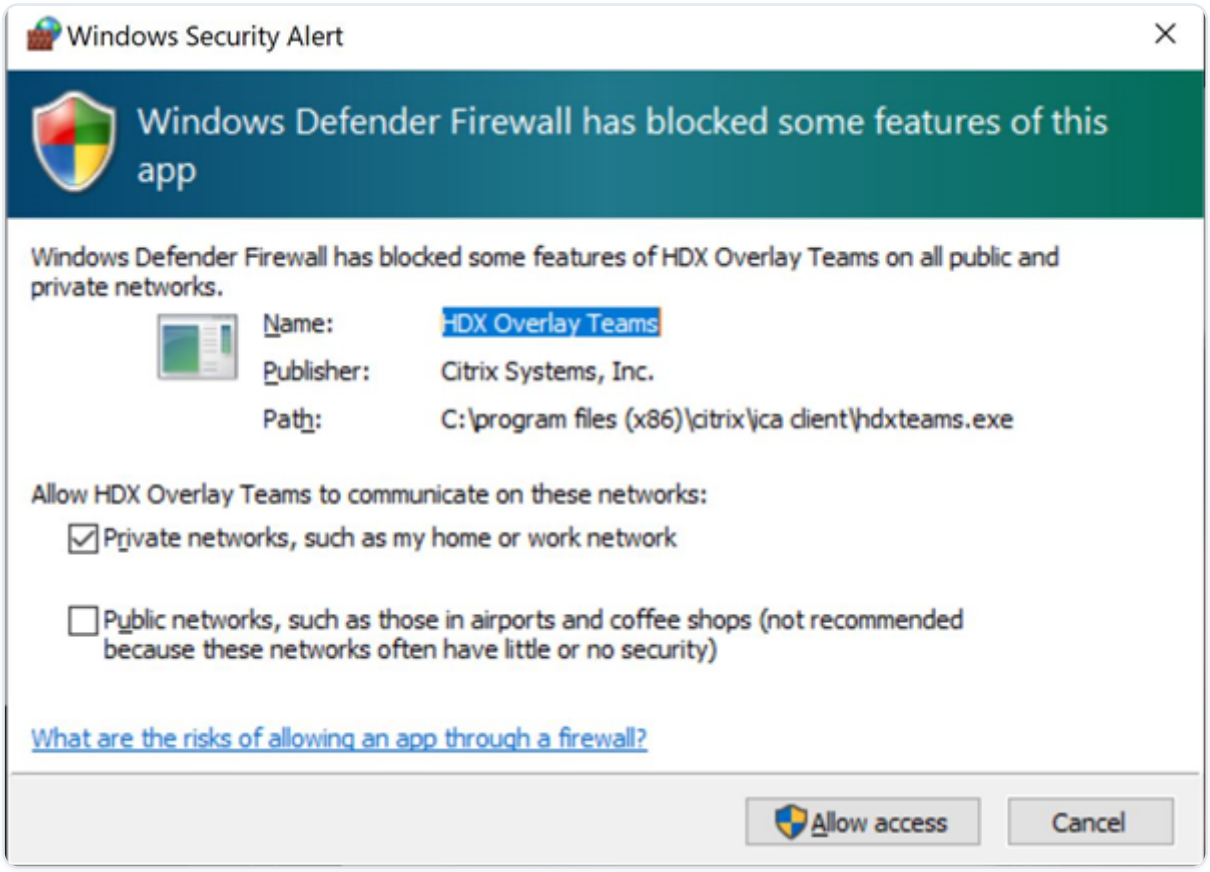
Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de localização despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

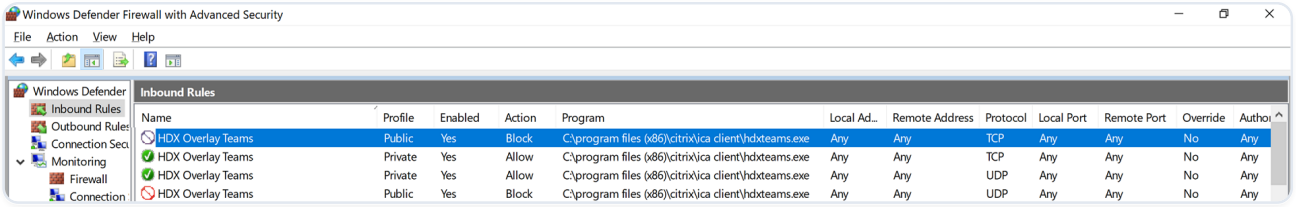
- ID do Chassi / ID da Porta usando o Protocolo de Descoberta da Camada de Link (LLDP) para conexões Ethernet/Switch. Ethernet/Switch (LLDP) é suportado em:
  - Versões do Windows 8.1 e 10
  - macOS, que requer software de habilitação LLDP. Para baixar o software de habilitação LLDP, vá para `www.microsoft.com` e procure por software de habilitação LLDP.
  - Linux, que requer que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do Thin Client.
- BBSID WLAN e {IPv4-IPv6; Sub-rede; Endereço MAC} do endpoint onde o aplicativo Citrix Workspace está instalado.
  - Locais baseados em sub-rede e WiFi são suportados no aplicativo Workspace para Windows, Linux e Mac.
- Latitude e Longitude, se a permissão do usuário for concedida no nível do sistema operacional onde o aplicativo Citrix Workspace está instalado (a permissão é definida como HDX RTC Engine)
  - Compatível com todas as plataformas do aplicativo Workspace. No entanto, para o Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do sistema operacional do Thin Client (>sudo apt-get install libgps23 gpsd lldpd).

## Considerações sobre firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso nas configurações do **firewall do Windows**. O aviso pede aos usuários que permitam a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).




As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Windows Defender Firewall > Segurança Avançada**. Você pode aplicar regras mais restritivas se desejar.



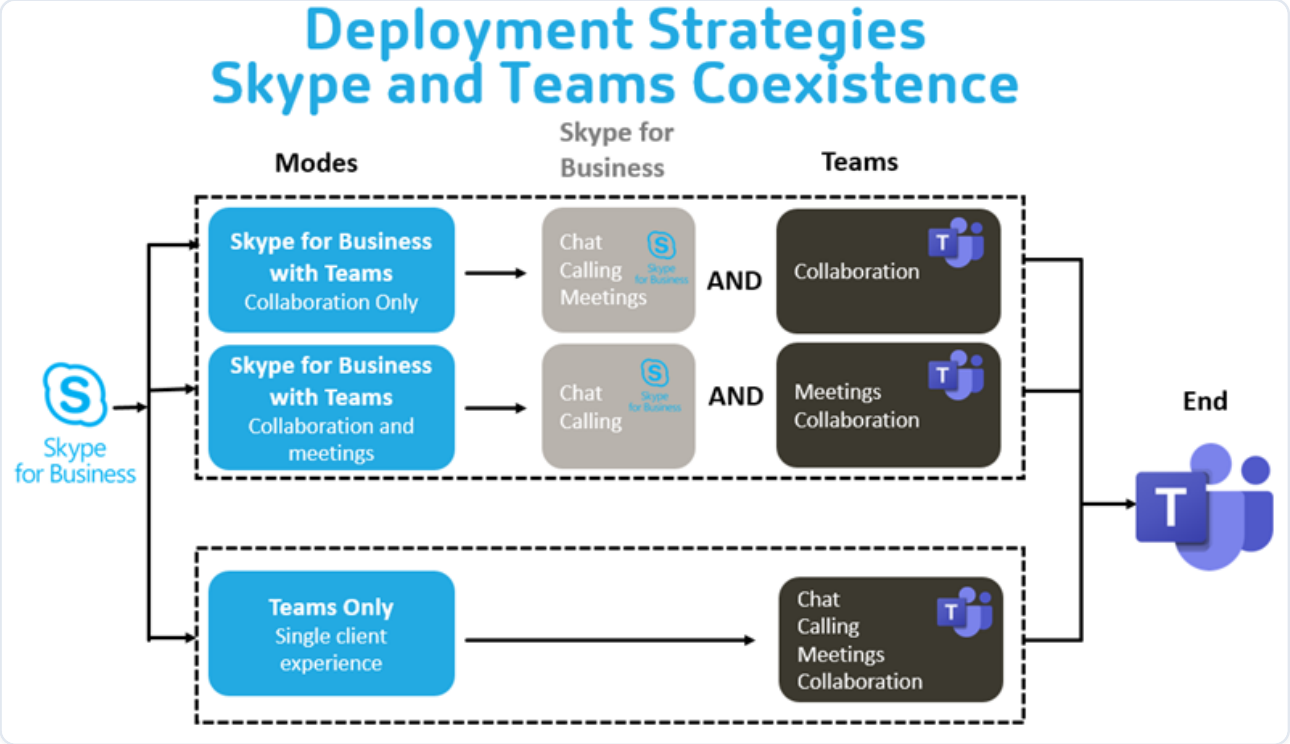

## Coexistência do Microsoft Teams e do Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado como duas soluções separadas com recursos sobrepostos. Para obter mais informações, consulte Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para mecanismos multimídia do Microsoft Teams, então, respeitam a configuração definida em seu ambiente. Os exemplos incluem modos de ilha e Skype for Business com colaboração do Microsoft Teams. Além disso, Skype for Business com colaboração e reuniões do Microsoft Teams.

O acesso a periféricos pode ser concedido a apenas um aplicativo por vez. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem

durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.




## Citrix SD-WAN™: conectividade de rede otimizada para Microsoft Teams

A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio e vídeo do Microsoft Teams de usuários do Citrix Workspace app em filiais para um data center antes de ir para a internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço web do Microsoft 365 baseado em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

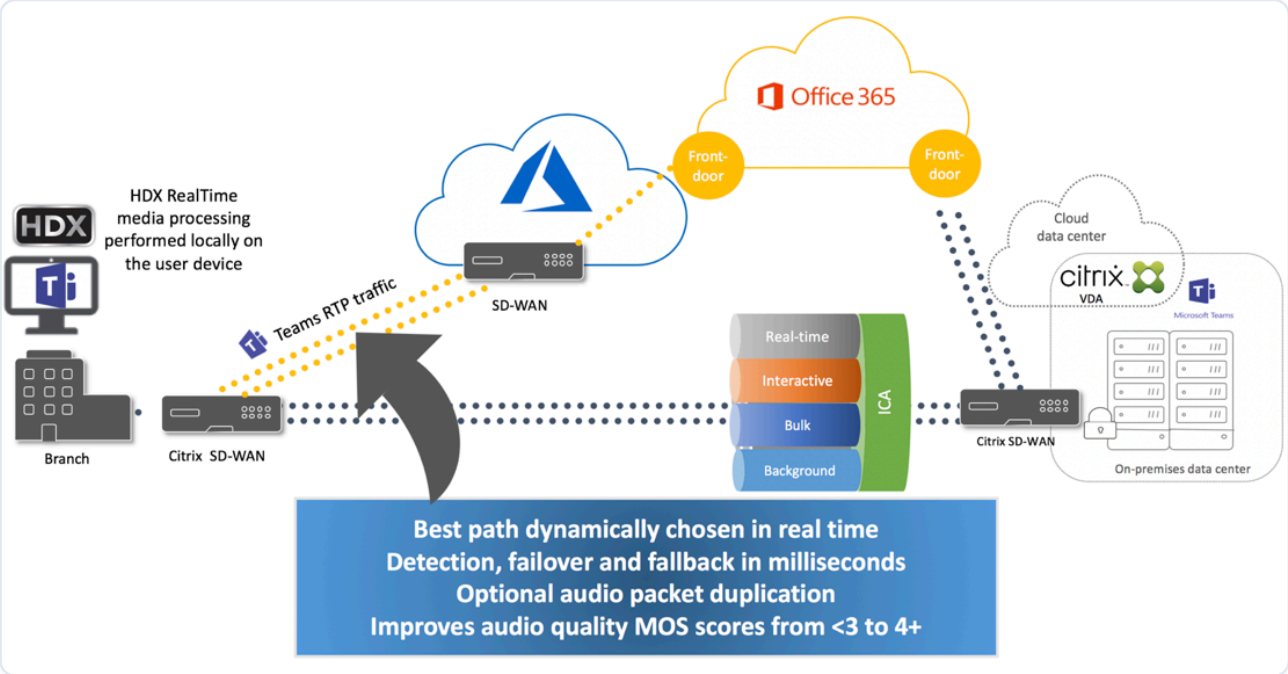
As conexões de internet banda larga empresarial em muitas áreas sofrem com perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio e vídeo do Microsoft Teams quando a integridade da rede é variável ou degradada.

- Se você usa o Microsoft Azure, um appliance virtual Citrix SD-WAN (VPX) implantado na VNET do Azure oferece otimizações avançadas de conectividade. Essas otimizações incluem failover de link contínuo e audio packet racing.

- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud™ Direct. Este serviço oferece entrega confiável e segura para todo o tráfego destinado à internet.

Se a qualidade da conexão de internet da filial não for uma preocupação, pode ser suficiente minimizar a latência. Direcione o tráfego do Microsoft Teams diretamente do appliance de filial do Citrix SD-WAN para o front door mais próximo do Microsoft 365 para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.




## Reuniões e bate-papo em várias janelas

Você pode usar várias janelas de reunião ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Janelas Pop-Out do Microsoft Teams para Bate-papos e Reuniões no site do Microsoft 365.

**Nota:**

Este recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Ele requer VDA 2112 ou superior e foi retroportado para 1912 CU6+ LTSR.

# Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 oferece suporte a desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas, ajudando a conversa a permanecer focada na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas P2P ou de conferência.

> **Nota:**
>
> Este recurso é integrado à interface do usuário/botões do Microsoft Teams. O suporte a MultiWindow é um pré-requisito que exige uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte Reuniões e bate-papo em várias janelas.
>
> Os controles da interface do usuário do Microsoft Teams para desfoque e efeitos de fundo exigem as seguintes versões mínimas:

- Aplicativo Citrix Workspace para Windows 2207
- Aplicativo Citrix Workspace para Mac 2301
- Aplicativo Citrix Workspace para Linux 2307
- Aplicativo Citrix Workspace para ChromeOS 2303

**Limitações:**

- O cliente deve estar conectado à internet ao substituir a imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição de imagem de fundo definida pelo administrador e pelo usuário não é suportada na interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser configuradas usando as configurações no cliente, se a imagem também estiver armazenada no cliente.

## Definindo uma imagem de fundo personalizada

As seguintes chaves de registro são necessárias apenas se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso, ou se um administrador deseja substituir comportamentos padrão. Por exemplo, desativar o desfoque de fundo porque o endpoint não é potente o suficiente.

### No Windows

Para definir uma imagem de fundo personalizada, administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou endpoint:

Local: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição de imagem de fundo)

Um valor definido como 1 desfoca o plano de fundo. O usuário final ou o administrador pode definir esse valor.

O valor definido como 2 também exige que a chave **VideoBackgroundImage** esteja presente. Somente o administrador pode definir este valor. A chave a seguir é necessária apenas se você deseja substituir a imagem de fundo e 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 de registro também pode ser usada para habilitar o desfoque de fundo ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de UI do Microsoft Teams. Em outras palavras, se seu ambiente ou VDA não suportar várias janelas, você ainda pode aplicar a solução alternativa de registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações na chave do registro só entram em vigor quando a sessão HDX se conecta.

### No Mac

Local da imagem baixada pelo usuário: */Users/username/Downloads/any_image.png*

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

`defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"`

**No Linux**

Local da imagem baixada pelo usuário: */home/username/Downloads/any_image.jpg*

Crie o arquivo */var/.config/citrix/hdx_rtc_engine/config.json* e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

**No HTML5**

1. navegar até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. Salve as alterações.

### Considerações sobre o consumo de CPU do cliente

Embora o recurso de desfoque seja econômico em termos de CPU, você pode esperar um aumento no consumo. Por exemplo, em um thin client com um chip Intel® Pentium® Silver de 4 núcleos, 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

## Visualização de galeria e oradores ativos no Microsoft Teams

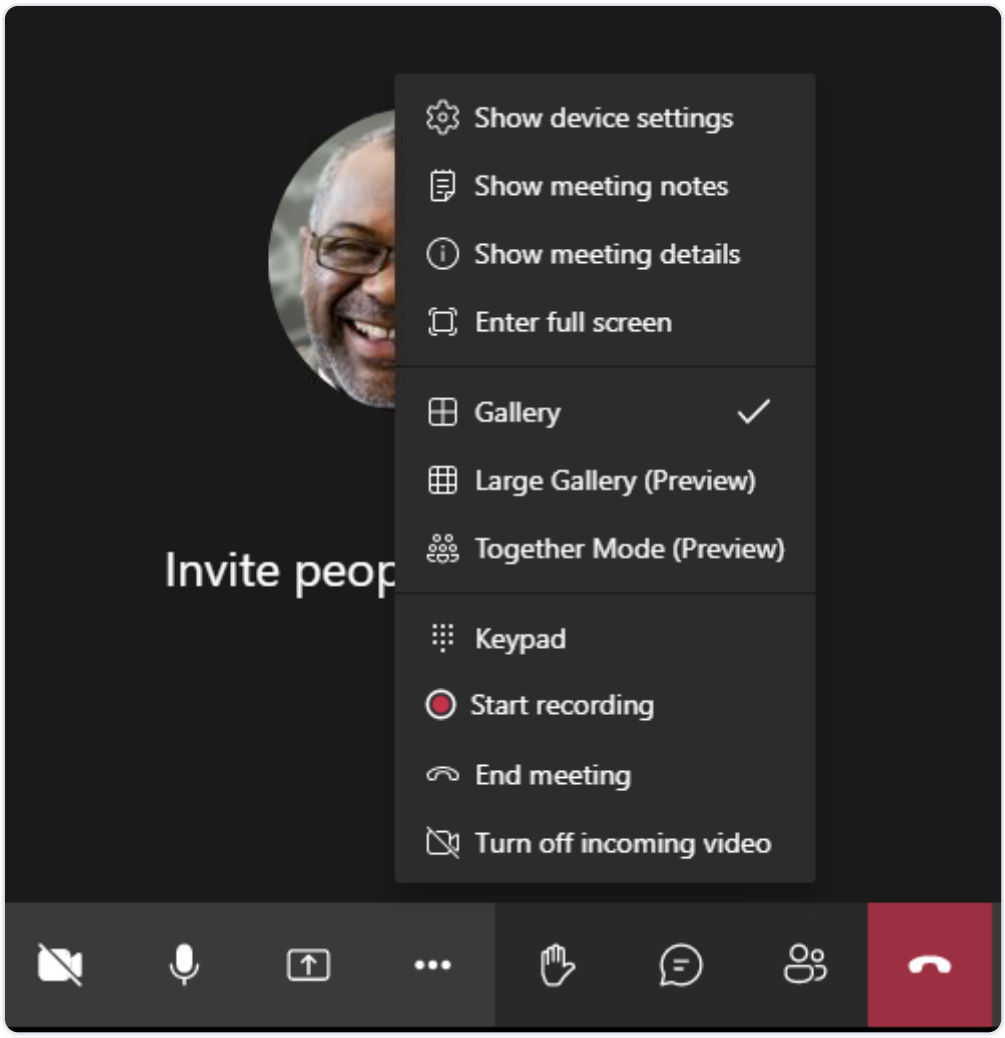
O Microsoft Teams oferece suporte aos layouts **Galeria**, **Galeria grande** e **Modo Juntos**.

O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecida como **Galeria**). Neste caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham um vídeo, apenas os últimos quatro oradores mais ativos aparecem na tela.

O Microsoft Teams também oferece a visualização de galeria grande com uma grade de até 7x7. Como resultado, o servidor de conferência do Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Este feed único, estilo matriz, também pode incluir vídeos de auto-visualização dos usuários.

Por fim, o Microsoft Teams oferece suporte ao **Modo Juntos**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para posicionar digitalmente os participantes em um plano de fundo compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada de conferência selecionando os layouts **Galeria**, **Galeria grande** ou **Modo Juntos** no menu de reticências.




Suporte para restrições de proporção de vídeo (aplicativo Citrix Workspace para Windows 2102, aplicativo Citrix Workspace para Linux 2106, aplicativo Citrix Workspace para MAC 2106 e posterior):

- A opção **Preencher para enquadrar** está disponível na Visualização de Galeria/Galeria Grande. Esta opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts de Galeria e Galeria Grande:

| | VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO) | VISUALIZAÇÃO DE GALERIA AMPLA |
|---|---|---|
| Layout / Grade | Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro oradores mais ativos aparecem na tela e outros | Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes. |

| | VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO) | VISUALIZAÇÃO DE GALERIA AMPLA |
|---|---|---|
| | participantes não aparecem na grade. | |
| Técnica de mixagem | Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário. | Um servidor de conferência central mixa e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Essa ação introduz alguma latência adicional. |
| Orador ativo | O novo orador ativo substitui o orador menos ativo na grade. | Exibe todos os participantes independentemente de estarem ativos ou inativos. |
| Codificação no endpoint | Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast. | Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast. |
| Decodificação no endpoint | Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no endpoint pelo HdxRtcEngine.exe (para decodificação/renderização). | Cada participante recebe apenas um único fluxo para áudio e vídeo. Essa configuração reduz o consumo de CPU no endpoint. |
| Resolução máxima | 720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é de 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando | 720p para o layout composto ou mixagem. Não há necessidade de um fluxo de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente |

| | VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO) | VISUALIZAÇÃO DE GALERIA AMPLA |
|---|---|---|
| | vídeo, a resolução por feed de vídeo pode ser maior. | reduz a resolução ou a taxa de bits de upload. |
| Problema de 'usuário lento' | O remetente modifica a qualidade de cada modalidade (áudio/vídeo/ compartilhamento de tela) para a menor qualidade de rede comum entre os participantes. Este fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com condição de rede ruim afeta a qualidade para todos os outros na chamada. | Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência oferece diferentes qualidades com base nas condições de rede dos participantes individuais. |
| Pré-visualização | Exibe você em uma pequena miniatura em tempo real. | Exibe você em miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout de vídeo principal com algum atraso adicional. |

## Compartilhamento de tela no Microsoft Teams

O Microsoft Teams depende do compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho compartilhada com codecs de vídeo como H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do Citrix Workspace app 2109 ou superior para Windows, Linux, Mac, e Citrix Workspace app 2303 para ChromeOS, os usuários podem compartilhar suas telas e câmera de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro participante começar a compartilhar a área de trabalho, o feed de vídeo original da câmera será pausado. Em

vez disso, o feed de vídeo de compartilhamento de tela é exibido. O participante deve então retomar manualmente o compartilhamento da câmera.

**Observação para o PowerPoint Live**

Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros participantes ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para revisar outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar um conjunto de slides do PowerPoint Live, clique no botão 'Share tray' e selecione um dos slides sugeridos do PowerPoint, ou clique em 'Browse' e encontre um arquivo do PowerPoint em seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Qualquer aplicativo local que se sobreponha ao Desktop Viewer não é capturado.

**Nota**

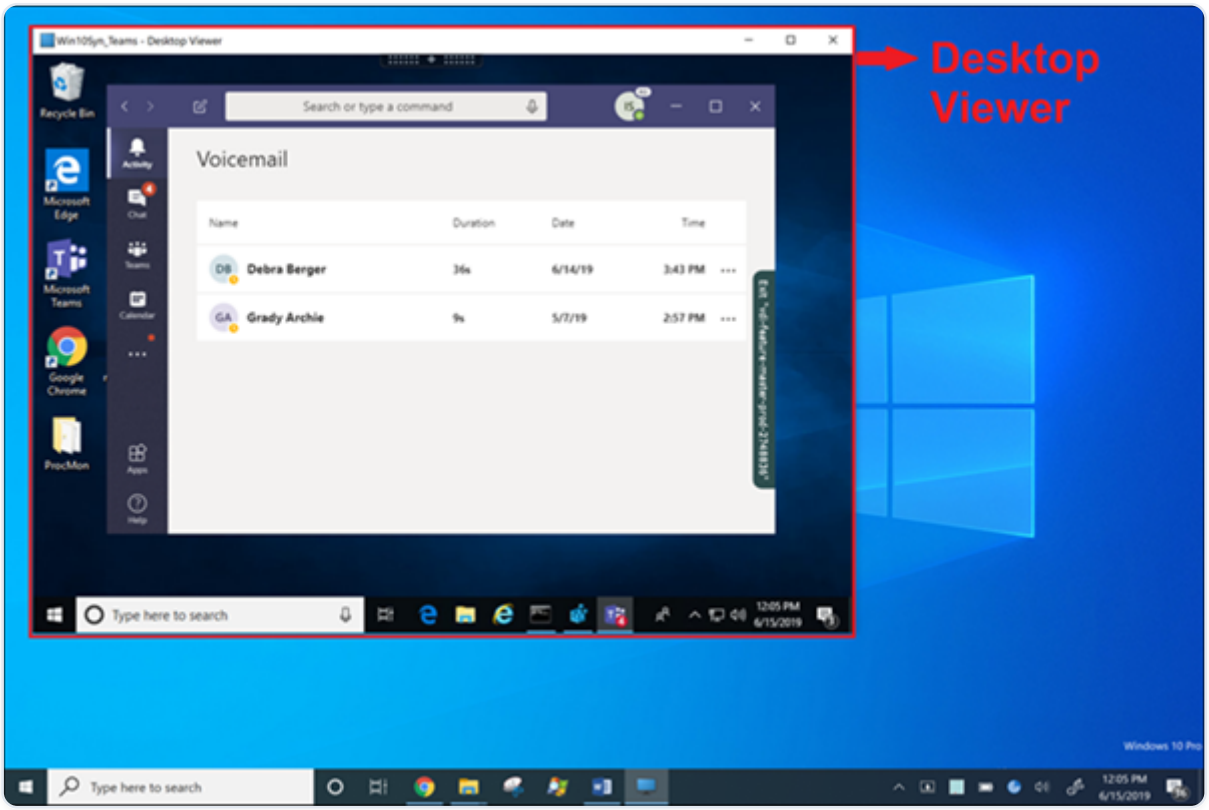
Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

**Limitação conhecida:**

- Se o Desktop Viewer estiver desabilitado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desabilitado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela em vários monitores.
- Em versões do aplicativo Workspace anteriores a 2106, apenas o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor principal para que os outros participantes da chamada possam vê-lo.
- O compartilhamento de tela em vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout de monitor virtual (partição lógica de um

único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.

- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento é possível apenas se o aplicativo local for sobreposto ao Desktop Viewer. Esse comportamento foi removido nas versões 2009.6 ou superior e 1912 CU5 ou superior.
- Durante o compartilhamento de tela, se você mudar do modo janela para tela cheia, o compartilhamento de tela para. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.
- Não é possível Fixar os Controles de Compartilhamento em um local específico no Microsoft Teams Otimizado.
- Ao compartilhar um aplicativo minimizado, a barra de título do aplicativo também pode ser compartilhada.




**Compartilhamento de tela de aplicativo contínuo:**

Se você estiver publicando o Microsoft Teams como um aplicativo autônomo e contínuo, o compartilhamento de tela capturará a área de trabalho local do seu endpoint físico. É necessária a versão mínima 1909 do aplicativo Citrix Workspace.

### Compartilhamento de apps

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

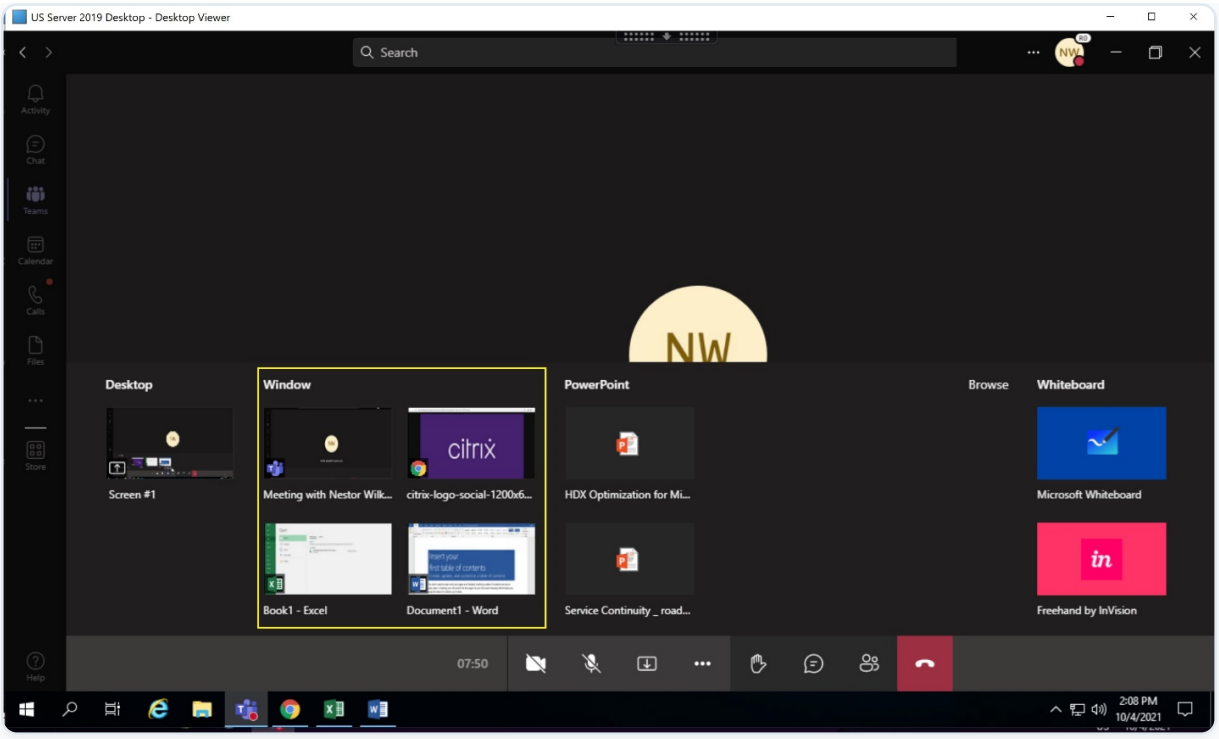
A partir do aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Você também pode compartilhar aplicativos internos personalizados, como Java, usando o Microsoft Teams otimizado. Para compartilhar um aplicativo específico:

1. navegar para o aplicativo Microsoft Teams dentro da sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo selecionado e os participantes da chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desabilitar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`: Nome: `UseWsProvider` Tipo: `DWORD` Valor: 0

> **Nota:**
>
> - Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
> - O compartilhamento de tela depende da captura da janela pelo lado do VDA. O conteúdo é então retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para o participante ou servidor de conferência.




**Limitações conhecidas com o compartilhamento de tela de aplicativos específicos:**

- O ponteiro do mouse não fica visível ao compartilhar a tela de um aplicativo.
- Se você minimizar um aplicativo enquanto o estiver compartilhando, apenas o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até que você maximize o aplicativo.
- Os aplicativos LAA mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de desktop no Microsoft Teams otimizado no VDA. No entanto, ao selecionar o aplicativo da lista, o resultado pode não ser o esperado.

**Compatibilidade com a proteção de aplicativos** O compartilhamento de tela de um aplicativo específico é compatível com o recurso de proteção de aplicativos no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico se tiver iniciado o aplicativo ou a área de trabalho de um grupo de entrega que tenha a proteção de aplicativos ativada.

Ao clicar em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Desktop**. Você só pode selecionar a opção **Janela** para compartilhar qualquer aplicativo aberto.

> **Nota:**

> Ao iniciar aplicativos ou áreas de trabalho de um grupo de entrega com proteção de aplicativo habilitada, você não consegue ver o vídeo ou o compartilhamento de tela recebidos se estiver usando o aplicativo Citrix Workspace para Windows 2202 ou anterior.

### Conceder e solicitar controle no Microsoft Teams

Este recurso é compatível com as seguintes versões do aplicativo Citrix Workspace (não há dependência da versão do VDA ou do Sistema Operacional, sessão única ou multissessão):

- Aplicativo Citrix Workspace para Windows versão 2112.1 ou posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 ou posterior
- Aplicativo Citrix Workspace para Linux versão 2203 ou posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2303 ou posterior

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de ter o controle, você pode fazer seleções, edições ou outras atividades de teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela estiver sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar sua solicitação.

Enquanto você tiver o controle, poderá fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar tanto um teclado quanto um mouse. Quando terminar, clique em **Solicitar controle**.

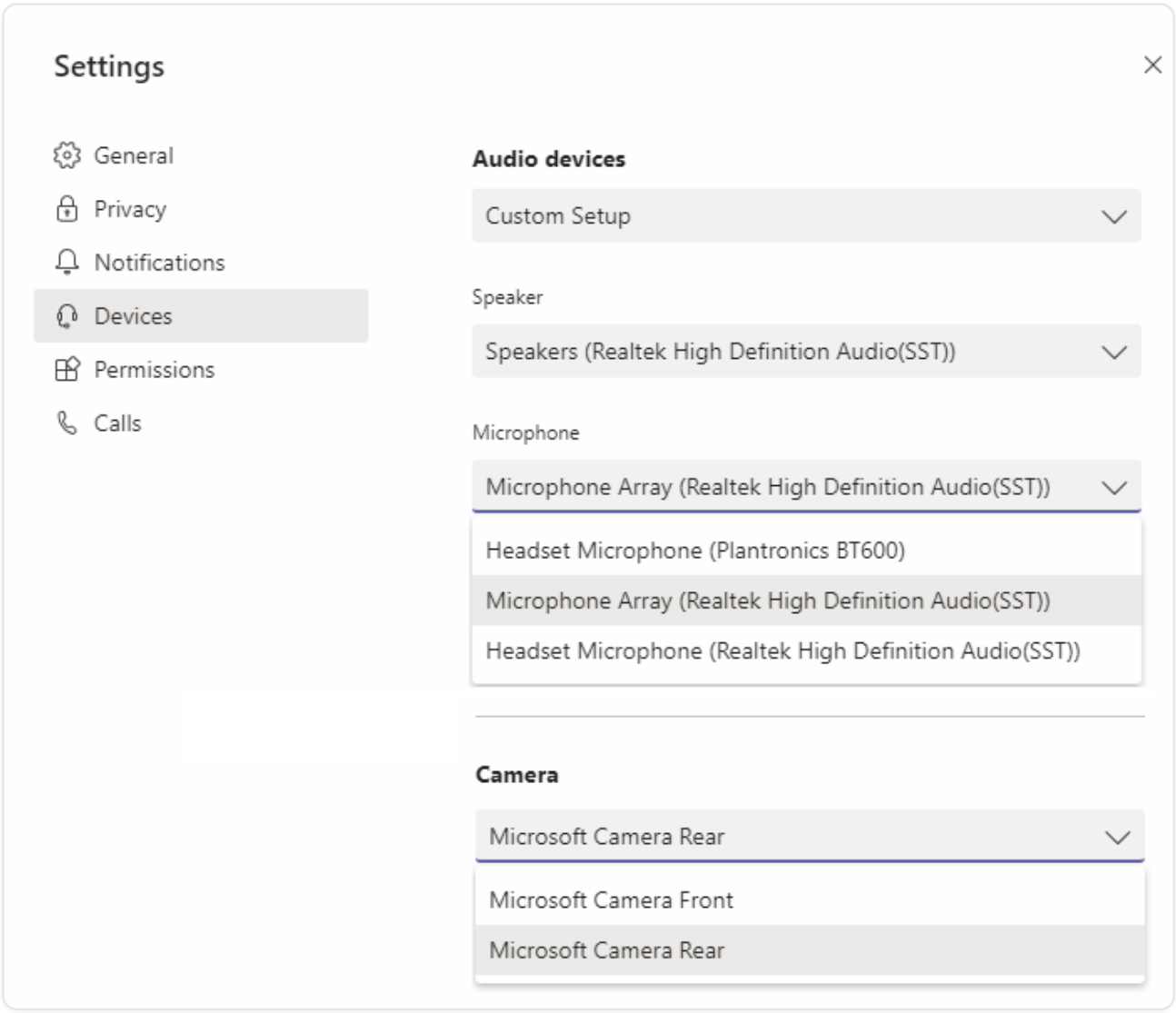
> **Limitações:**

> - Os controles de Conceder e Solicitar não estão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como Compartilhamento de aplicativo). A área de trabalho ou o monitor completo deve ser compartilhado.
> - O recurso para fixar a barra de controle em um local específico não está disponível.

## Periféricos no Microsoft Teams

Quando a otimização para Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fones de ouvido, microfones, câmeras, alto-falantes e assim por diante). Então, os

periféricos são listados corretamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).




O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele depende do mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você deve selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão do mesmo endpoint.

**Recomendações:**

- Fones de ouvido certificados para Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde o microfone e os alto-falantes estão em

dispositivos separados, pode haver eco. Um exemplo é uma webcam com microfone integrado e um monitor com alto-falantes. Ao usar alto-falantes externos, 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` e procure por fones de ouvido certificados para Microsoft Teams.

- Câmeras certificadas para Microsoft Teams, embora os periféricos certificados para Skype for Business sejam compatíveis com o Microsoft Teams. Para obter mais informações, acesse <www.microsoft.com> e procure por câmeras certificadas para Microsoft Teams e periféricos certificados para Skype for Business.
- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento da CPU com webcams que realizam codificação H.264 integrada - UVC 1.1 e 1.5.

**Nota:**

O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio de 24 bits ou com frequências acima de 96 kHz.

HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou anterior) suporta apenas estes formatos específicos de dispositivo de áudio (canais, profundidade de bits e taxa de amostragem):

- Dispositivos de Reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
- Dispositivos de Gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz

Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.

Os logs do **Webrpc** em **HdxTeams.exe** mostram este tipo de informação:

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

> `Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

> Como solução alternativa, desative o dispositivo específico ou:

> 1. Abra o **Painel de Controle de Som** (mmsys.cpl).
> 2. Selecione o dispositivo de reprodução ou gravação.
> 3. Vá para **Propriedades > Avançado** e altere as configurações para um modo compatível.

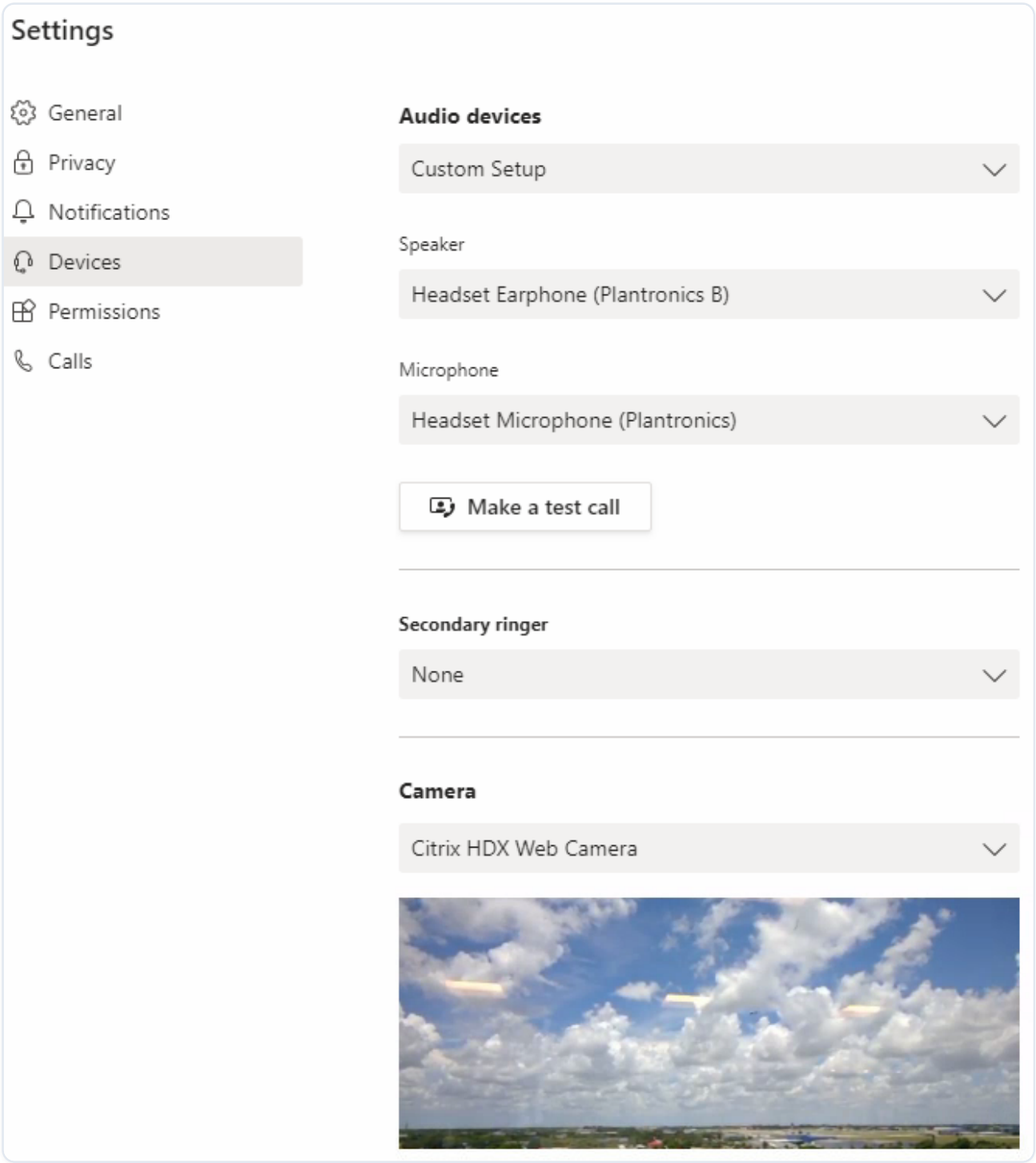
### Modo de fallback

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Not Connected" em Microsoft Teams/Sobre/Versão), o VDA retorna às tecnologias HDX legadas. As tecnologias HDX legadas podem ser redirecionamento de webcam e redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão/plataforma de SO do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam. No modo de fallback, os periféricos são mapeados para o VDA. Os periféricos aparecem para o aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no VDA. Para obter mais informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados por meio do registro.

Este recurso requer a versão 1.3.0.13565 ou posterior do Microsoft Teams.

Para determinar se você está no modo otimizado ou não otimizado ao olhar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX legadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX**, conforme mostrado na imagem a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) em comparação com o modo otimizado.




Quando tecnologias HDX legadas são usadas, o Microsoft Teams não descarrega o processamento de áudio, vídeo e compartilhamento de tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do endpoint. Em vez disso, as tecnologias HDX usam renderização do lado do servidor. Espere alto consumo de CPU no VDA ao ligar o vídeo. O desempenho de áudio em tempo real pode não ser ideal.

# Limitações conhecidas

## Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- As configurações de QoS no Centro de Administração para Microsoft Teams não se aplicam a usuários VDI.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo poderá ser capturado.

Limitação no VDA:

- Quando você configura a definição **Citrix Workspace app High DPI** para `Yes`, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente — não no VDA.

## Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams no Windows e Mac. Para Linux, verifique com o fornecedor do seu thin client. Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes endpoints são aprimoradas, adaptando-se à resolução adequada para a melhor experiência de chamada para todos os participantes.

Com esta experiência aprimorada, cada usuário pode entregar múltiplos fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p, e assim por diante) dependendo de vários fatores, incluindo a capacidade do endpoint, condições de rede, e assim por diante. O endpoint receptor então solicita a resolução de qualidade máxima que ele pode manipular, proporcionando assim a todos os usuários a experiência de vídeo ideal.

> **Nota:**

> Este recurso está disponível somente após o lançamento de uma atualização do Microsoft Teams. Para obter informações sobre a ETA, vá para `<https://www.microsoft.com/>` e procure por roteiro do Microsoft 365. Quando a atualização for lançada pela Microsoft, você pode verificar CTX253754 para a atualização da documentação e o anúncio.

### Limitações da Microsoft

- A visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams – entre em contato com a Microsoft para saber quando esperar uma grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.
- A resolução máxima do fluxo de vídeo de entrada e saída é 720p.
- O tom de retorno de chamada PSTN não é suportado.
- O desvio de mídia para Roteamento Direto não é suportado.
- As funções de produtor e apresentador de transmissão e evento ao vivo não são suportadas. A função de participante é suportada, mas não otimizada (renderiza no VDA).
- A função de zoom in e zoom out no Microsoft Teams não é suportada.
- O Roteamento Baseado em Localização e o Desvio de Mídia não são suportados.
- A fusão de chamadas não é suportada (opção não exibida na interface do usuário).

### Limitações da Citrix e da Microsoft

- Ao compartilhar a tela, a opção **incluir áudio do sistema** não está disponível.
- Simulcast não é suportado no ChromeOS.

## Próximo EOL do Microsoft Teams de Janela Única

Em January 31, 2024, a Microsoft descontinuará o suporte do Microsoft Teams para a interface de usuário de janela única ao usar a otimização do Microsoft Teams VDI e suportará apenas a experiência de múltiplas janelas. A Microsoft notificou essa descontinuação em 9/8/2023 no Centro de Administração do M365 (ID da Postagem: MC674419). Detalhes públicos sobre o recurso de múltiplas janelas podem ser encontrados no artigo da Tech Community: New Meeting and Calling Experience in Microsoft Teams.

> **Observação:**

A Citrix recomenda que você atualize seu VDA e o aplicativo Citrix Workspace para as versões suportadas para continuar usando o Microsoft Teams no modo otimizado para vídeo e compartilhamento de tela. Se você não atualizar sua infraestrutura e endpoints para suportar múltiplas janelas, suas chamadas, chamadas de vídeo e compartilhamento de tela se tornarão não otimizados. Isso pode resultar em problemas de qualidade de chamada, aumento da latência e aumento da carga no servidor.

A tabela a seguir ilustra as versões mínima, LTSR e recomendada do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams em Citrix VDI:

| COMPONENTE | VERSÃO MÍNIMA (1) | VERSÃO SUPORTADA 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+ |
| 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+ |

**Observações:**

1. Versão Mínima: Esta é a versão onde o Multi-window foi introduzido pela primeira vez. Algumas versões mínimas listadas aqui podem estar no fim da vida útil.
2. Versão LTSR Suportada: Esta é a versão LTSR que é suportada pela Citrix para Multi-window. Versões mais antigas dessas edições LTSR podem funcionar, mas o suporte não está mais disponível para essas versões assim que uma nova versão LTSR CU é lançada. Para mais informações sobre as políticas de suporte LTSR, consulte `<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`.
3. Versão Recomendada: Esta é a versão do software que a Citrix recomenda se o usuário/cliente optar por atualizar seu software. Todas estas são versões CR.
4. A versão 2203 LTSR para VDA e as versões base do CWA incluem a funcionalidade de multi-janela. Estas versões foram substituídas pela CU mais recente, que é a versão oficialmente suportada. Os clientes podem continuar a usar estas versões não suportadas a seu critério. A Citrix incentiva os clientes na versão LTSR a atualizar para a CU mais recente.

## Anúncio de descontinuação do formato SDP (Plano B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP atual (Plano B) do WebRTC em futuras versões. Você deve usar o Plano Unificado no WebRTC para oferecer suporte às funcionalidades otimizadas do Microsoft Teams.

### Produtos afetados

Em uma das futuras versões do Citrix Workspace Application, chamadas entre endpoints com a próxima versão do aplicativo Citrix Workspace e endpoints com o aplicativo Citrix Workspace 2108 ou versões mais antigas não serão suportadas. Essa incompatibilidade de chamada inclui clientes do aplicativo Citrix Workspace 1912 LTSR (CWA). Os seguintes clientes CWA são afetados:

- Citrix Workspace app para Windows
- Citrix Workspace app para Linux
- Citrix Workspace app para Mac
- Citrix Workspace app para Chrome

### Substituição para o Plano B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior a 2109, você deve atualizar para uma versão suportada (preferencialmente a última versão CR). Caso contrário, quaisquer chamadas com uma versão futura ou endpoints mais recentes falharão ao conectar. Chamadas entre versões futuras e seus parceiros de comunicação federados também podem falhar se o parceiro federado não tiver atualizado seu Citrix Workspace.

A versão 2108 do aplicativo Citrix Workspace completou sua data de suporte em março de 2023 e deve ser atualizada para uma versão mais recente. Para mais informações, consulte Workspace App para detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para mais informações sobre a descontinuação do Plano B, consulte a documentação WebRTC.

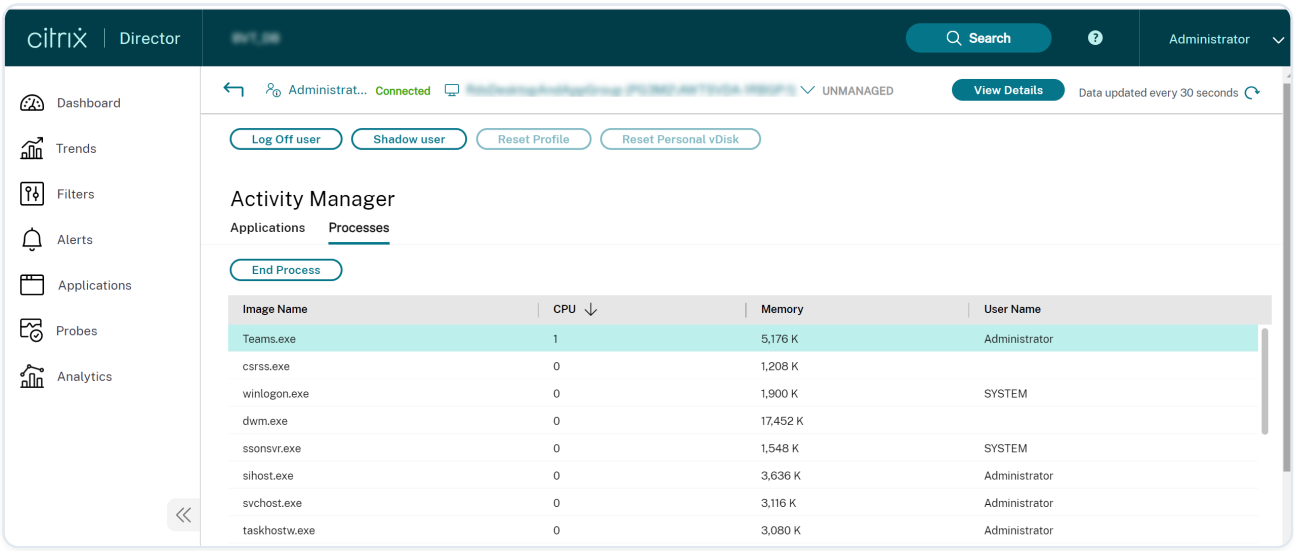
## Informações adicionais

- Monitorar, solucionar problemas e dar suporte ao Microsoft Teams
- Implantar o aplicativo de desktop do Microsoft Teams na VM
- Instalar o Microsoft Teams usando MSI (seção Instalação VDI)
- Thin clients
- Ferramenta de Avaliação de Rede do Skype for Business
- Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business

## Monitorar, solucionar problemas e oferecer suporte ao Microsoft Teams

### Monitorar o Teams

Esta seção fornece diretrizes para monitorar a otimização do Microsoft Teams com HDX. Se você estiver executando no modo otimizado e `HdxRtcEngine.exe` estiver sendo executado na máquina cliente, um processo no VDA chamado `WebSocketAgent.exe` estará sendo executado na sessão. Use o **Activity Manager** no Director para ver o aplicativo.




O status de otimização do Microsoft Teams pode ser visualizado na página Director > **User Details** > painel **Session Details** > campo **MS Teams Optimization**. A otimização do Microsoft Teams é fundamental para uma melhor experiência do usuário, como áudio e vídeo nítidos. Este recurso está disponível para VDA versão 2311 e posterior. As versões do aplicativo Citrix Workspace™ suportadas estão listadas em Otimização para Microsoft Teams. O Director exibe o status da otimização do Microsoft Teams somente se o Microsoft Teams estiver sendo executado como um aplicativo publicado ou dentro de um desktop publicado. Para obter mais informações, consulte status de otimização do Microsoft Teams.

Com a versão mínima do VDA 1912, você pode monitorar chamadas ativas do Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`. Com a versão mínima do VDA 1912, você pode monitorar chamadas ativas do Microsoft Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`.

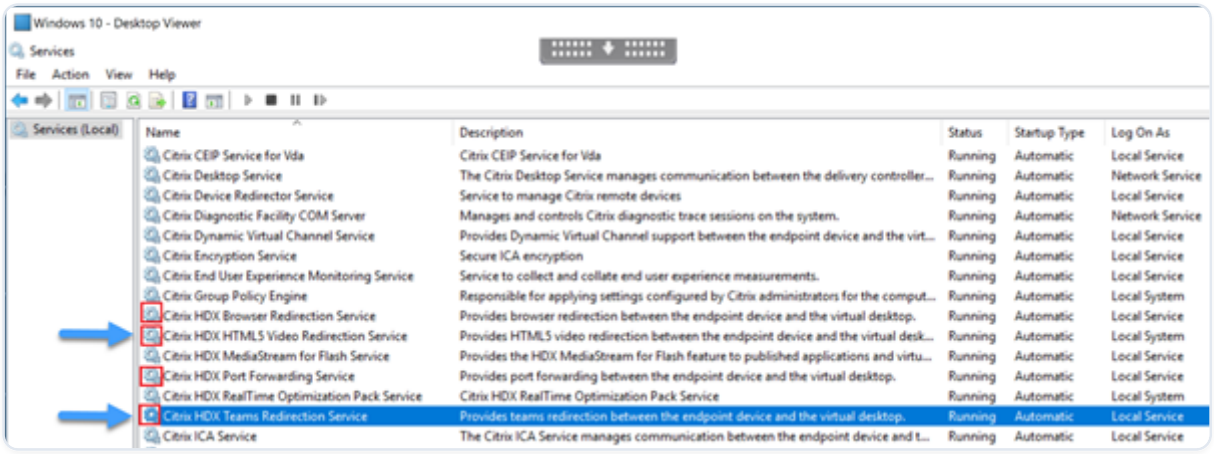
Para obter mais informações, consulte *Monitoramento* no artigo da Central de Conhecimento CTX253754.

## Solução de problemas

Esta seção fornece dicas de solução de problemas para questões que você pode encontrar ao usar a otimização para Microsoft Teams. Para obter mais informações, consulte CTX253754.

### No Virtual Delivery Agent

Existem quatro serviços instalados por BCR_x64.msi. Apenas dois são responsáveis pelo redirecionamento do Microsoft Teams no VDA.



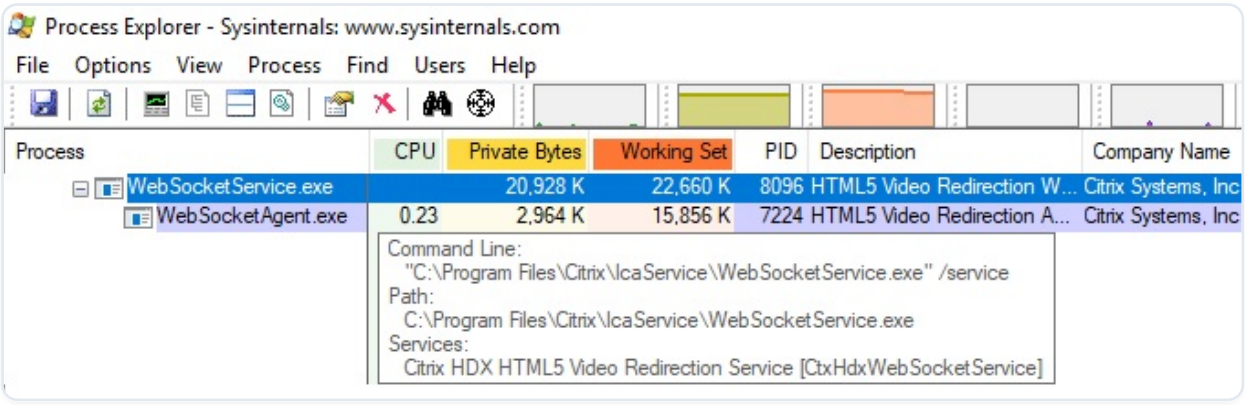

- **Serviço de Redirecionamento do Citrix HDX Teams** estabelece o canal virtual usado no Microsoft Teams. O serviço depende de CtxSvcHost.exe.
- O **Citrix HDX HTML5 Video Redirection Service** é executado como WebSocketService.exe, escutando em 127.0.0.1:9002 TCP. WebSocketService.exe executa duas funções principais:

  i. A **terminação TLS para WebSockets seguros** recebe uma conexão WebSocket segura de vdiCitrixPeerConnection.js, que é um componente dentro do aplicativo Microsoft Teams. Você pode rastreá-lo com o Process Monitor. Para obter mais informações sobre certificados, consulte a seção "Redirecionamento de vídeo TLS e HTML5 e redirecionamento de conteúdo do navegador" em Comunicação entre Controller e VDA.

  Alguns softwares antivírus e de segurança de desktop interferem no funcionamento adequado de `WebSocketService.exe` e seus certificados. Embora o serviço Citrix HDX HTML5 Video Redirection possa estar em execução no console `services.msc`, o socket TCP localhost `127.0.0.1:9002` nunca está no modo de escuta, como visto no netstat. Tentar reiniciar o serviço faz com que ele trave ("Parando..."). Certifique-se de aplicar as exclusões apropriadas para o processo `WebSocketService.exe`.




  ii. **Mapeamento de sessão do usuário.** Quando o aplicativo Microsoft Teams é iniciado, o WebSocketService.exe inicia o processo WebSocketAgent.exe na sessão do usuário no VDA. O WebSocketService.exe é executado na Sessão 0 como uma conta LocalSystem.




Você pode usar `netstat` para verificar se o serviço WebSocketService.exe está em um estado de escuta ativa no VDA.

Execute `netstat -anob -p tcp` a partir de uma janela de prompt de comando elevada:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

Em uma conexão bem-sucedida, o estado muda para ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

**Importante:**

O WebSocketService.exe escuta em dois soquetes TCP, 127.0.0.1:9001 e 127.0.0.1:9002. A porta 9001 é usada para redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5. A porta 9002 é usada para redirecionamento do Microsoft Teams. Certifique-se de não ter nenhuma configuração de proxy no sistema operacional Windows do VDA que possa impedir uma comunicação direta entre Teams.exe e WebSocketService.exe. Às vezes, ao configurar um proxy explícito no Internet Explorer 11 (**Opções da Internet > Conexões > Configurações da LAN > Servidor proxy**), as conexões podem fluir por um servidor proxy atribuído. Verifique se **Ignorar servidor proxy para endereços locais** está marcado ao usar uma configuração de proxy manual e explícita.

### Localizações e descrições de serviços

| SERVIÇO | CAMINHO PARA O EXECUTÁVEL NO SO WINDOWS SERVER | FAZER LOGON COMO | DESCRIÇÃO |
|---|---|---|---|
| Serviço de Redirecionamento de Vídeo HTML5 da Citrix | "C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service | Conta do Sistema Local | Fornece vários serviços multimídia HDX com a estrutura inicial necessária para realizar o redirecionamento de mídia entre o desktop virtual e o dispositivo de endpoint. |
| Serviço de Redirecionamento de Navegador Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs | Esta conta (serviço local) | Fornece redirecionamento de conteúdo do navegador entre o dispositivo de endpoint e o desktop virtual. |
| Serviço de Encaminhamento de Porta Citrix | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | Esta conta (serviço local) | Fornece encaminhamento de porta entre o dispositivo de endpoint e o desktop virtual para redirecionamento de conteúdo do navegador. |
| Serviço de Redirecionamento de Teams Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | Conta do Sistema Local | Fornece redirecionamento do Microsoft Teams entre o dispositivo de endpoint e o desktop virtual. |

### Aplicativo Citrix Workspace

No endpoint do usuário, o aplicativo Citrix Workspace para Windows instancia um novo serviço chamado HdxTeams.exe ou HdxRtcEngine.exe. Ele faz isso quando o Microsoft Teams é iniciado no VDA e o usuário tenta ligar ou acessar os periféricos na visualização automática. Se você não vir este serviço, verifique o seguinte:

1. Certifique-se de ter instalado no mínimo a Workspace App versão 1905 para Windows. Você vê os binários HdxTeams.exe ou HdxRtcEngine.exe e webrpc.dll no caminho de instalação do aplicativo Workspace?
2. Se você validou a etapa 1, faça o seguinte para verificar se HdxTeams.exe ou HdxRtcEngine.exe está sendo iniciado.
    a. Saia do Microsoft Teams no VDA.
    b. Inicie services.msc no VDA.
    c. Pare o Serviço de Redirecionamento do Citrix HDX Teams.
    d. Desconecte a sessão ICA®.
    e. Conecte a sessão ICA.
    f. Inicie o Serviço de Redirecionamento do Citrix HDX Teams.
    g. Reinicie o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX.
    h. Inicie o Microsoft Teams no VDA.
3. Se você ainda não vir HdxTeams.exe ou HdxRtcEngine.exe sendo iniciado no endpoint do cliente, faça o seguinte:
    a. Reinicie o VDA.
    b. Reinicie o endpoint do cliente.

## Suporte

A Citrix e a Microsoft dão suporte conjunto à entrega do Microsoft Teams a partir do Citrix Virtual Apps and Desktops™ usando a otimização para Microsoft Teams. Esse suporte conjunto é o resultado de uma colaboração estreita entre as duas empresas. Se você tiver contratos de suporte válidos e encontrar um problema com esta solução, abra um tíquete de suporte com o fornecedor cujo código você suspeita estar causando o problema. Ou seja, a Microsoft para o Teams ou a Citrix para os componentes de otimização. A Citrix ou a Microsoft recebe o tíquete, avalia o problema e o encaminha conforme apropriado. Não há necessidade de você entrar em contato com a equipe de suporte de cada empresa.

Quando tiver um problema, recomendamos que você clique em **Ajuda > Relatar um Problema** na interface do usuário do Teams. Os logs do lado do VDA são compartilhados automaticamente entre a Citrix e a Microsoft para resolver problemas técnicos mais rapidamente.

### Coletando logs

Os logs do mecanismo de mídia HDX podem ser encontrados na máquina do usuário (não no VDA). Em caso de problemas, certifique-se de anexar os logs ao seu caso de suporte.

**Logs do Windows:**

Você pode localizar os logs do Windows em %TEMP% dentro da pasta **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Procure por um arquivo .txt chamado webrpc_Day_Month_timestamp_Year.txt. Se você estiver usando versões mais recentes do aplicativo Citrix Workspace, por exemplo, Citrix Workspace app 2009.5 ou posterior, armazene os logs em AppData\Local\Temp\HdxRtcEngine.

Cada sessão cria uma pasta separada para os logs.

**Logs do Mac:**

1. Log VDWEBRTC - registra a execução do canal virtual.

   Localização: `/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`
2. Log HdxRtcEngine - registra a execução dos processos no HdxRtcEngine.

   Local: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   O log HdxRtcEngine é ativado por padrão.
3. Logs Webrpc - são os logs mais importantes que registram a execução do encerramento da biblioteca webrtc.

   Local: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

**Logs do Linux:**

Você pode localizar os logs do Linux nas pastas `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`. Log Webrtc: `/tmp/webrpc/<current date>/webrtc.log` Log do kernel: `/var/log/syslog`

**Logs ICE/STUN/TURN:**

Ao estabelecer uma chamada, estas quatro fases ICE são necessárias:

- Coleta de candidatos
- troca de candidatos
- Verificações de conectividade (solicitações de vinculação STUN)
- Promoção de candidatos

Nos logs do HdxRtcEngine.exe, as seguintes entradas são as entradas relevantes do Interactive Connectivity Establishment (ICE). Essas entradas devem estar presentes para que a configuração de uma chamada seja bem-sucedida. Consulte o seguinte trecho de exemplo para a fase de coleta:

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
```

```
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

Se houver vários candidatos ICE, a ordem de preferência é:

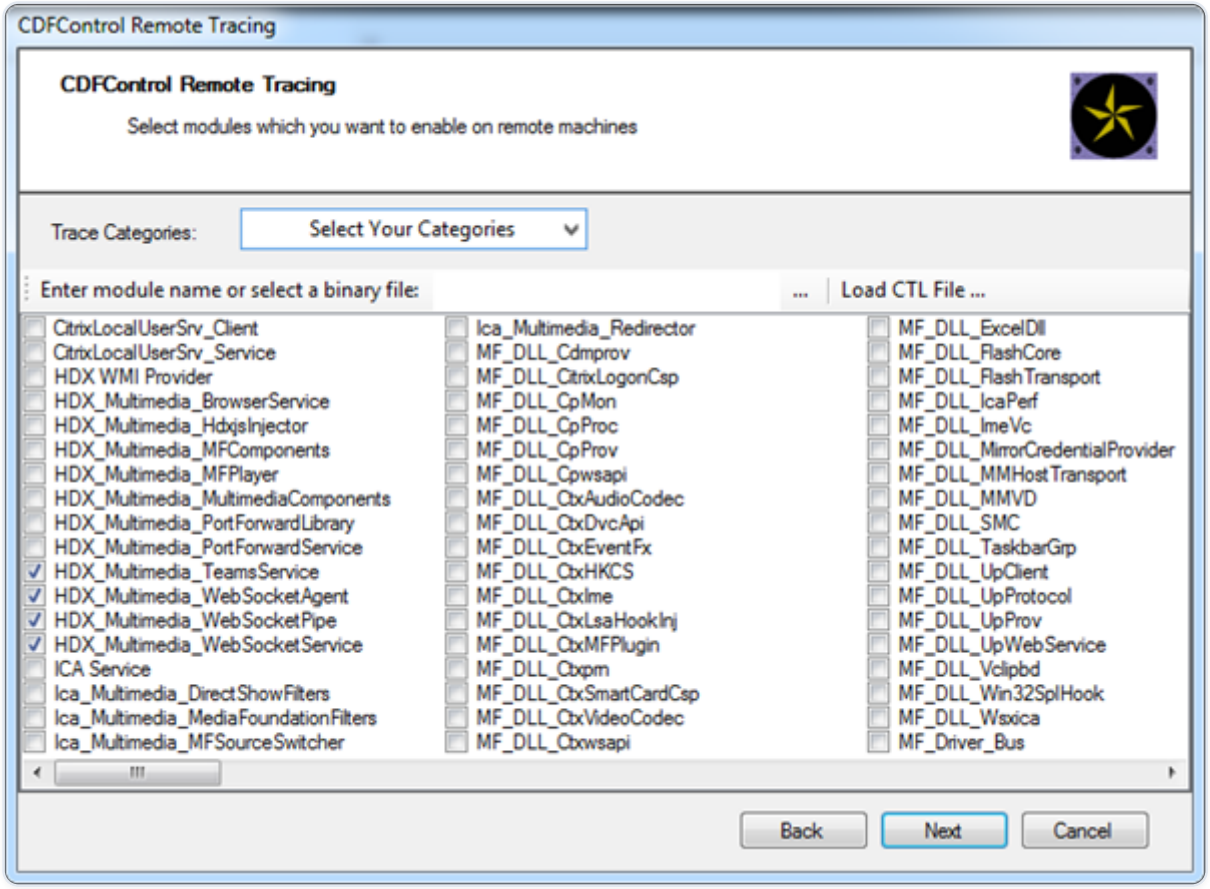
1. máquina

2. reflexivo de par
3. reflexivo do servidor
4. retransmissão de transporte

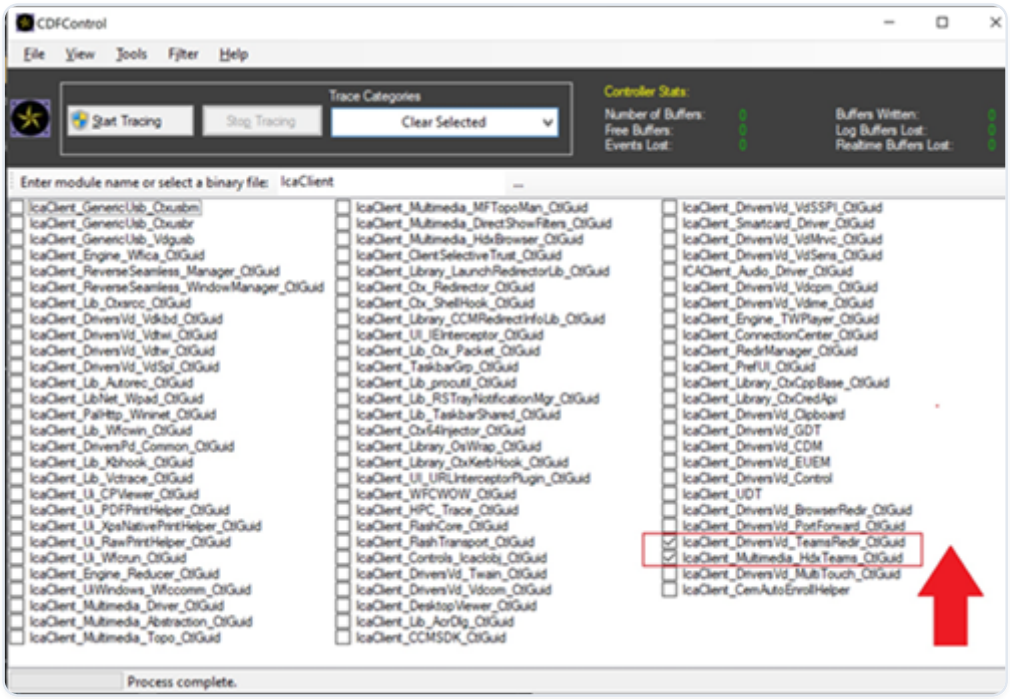
Se você encontrar um problema e puder reproduzi-lo consistentemente, recomendamos que clique em **Ajuda > Relatar um problema** no Microsoft Teams. Os logs são compartilhados entre a Citrix e a Microsoft para resolver problemas técnicos, caso você tenha aberto um caso com a Microsoft. A captura de rastreamentos CDF antes de entrar em contato com o Suporte Citrix também é benéfica. Para obter mais informações, consulte o artigo da Central de Conhecimento CDFcontrol.

Para recomendações sobre a coleta de rastreamentos CDF, consulte o artigo da Central de Conhecimento Recomendações para Coletar os Rastros CDF.

**Rastreamentos CDF do lado do VDA - Habilite os seguintes provedores de rastreamento CDF:**




**Rastreamentos CDF do lado do aplicativo Workspace - Habilite os seguintes provedores de rastreamento CDF:**




- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requer aplicativo Citrix Workspace 2012 ou posterior)

## Redirecionamento de Mídia do Windows

O redirecionamento de Mídia do Windows controla e otimiza a forma como os servidores entregam áudio e vídeo de streaming aos usuários. Ao reproduzir os arquivos de tempo de execução de mídia no dispositivo cliente em vez do servidor, o redirecionamento de Mídia do Windows reduz os requisitos de largura de banda para a reprodução de arquivos multimídia. O redirecionamento de Mídia do Windows melhora o desempenho do Windows Media Player e de players compatíveis executados em desktops virtuais do Windows.

Se os requisitos para a busca de conteúdo do lado do cliente do Windows Media não forem atendidos, a entrega de mídia usará automaticamente a busca do lado do servidor. Este método é transparente para os usuários. Você pode usar o Citrix Scout para realizar um rastreamento do Citrix Diagnosis Facility (CDF) de HostMMTransport.dll para determinar o método usado. Para obter mais informações, consulte Citrix Scout.

O redirecionamento de Mídia do Windows intercepta o pipeline de mídia no servidor host, captura os dados de mídia em seu formato compactado nativo e redireciona o conteúdo para o dispositivo cliente. O dispositivo cliente então recria o pipeline de mídia para descompactar e renderizar os dados de mídia recebidos do servidor host. O redirecionamento de Mídia do Windows funciona bem em dispositivos cliente que executam um sistema operacional Windows. Esses dispositivos possuem a estrutura multimídia necessária para reconstruir o pipeline de mídia como existia no

servidor host. Clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento de Mídia do Windows** controla este recurso e é **Permitido** por padrão. Geralmente, essa configuração aumenta a qualidade de áudio e vídeo renderizada do servidor para um nível comparável ao conteúdo reproduzido localmente em um dispositivo cliente. Em casos raros, a reprodução de mídia usando o redirecionamento de Mídia do Windows parece pior do que a mídia renderizada usando compressão ICA® básica e áudio regular. Você pode desabilitar este recurso adicionando a configuração **Redirecionamento de Mídia do Windows** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações de política, consulte Configurações de política de multimídia.

**Limitação:**

Ao usar o Windows Media Player e as Extensões de Áudio e Vídeo Remoto (RAVE) ativadas em uma sessão, uma tela preta pode aparecer. Esta tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Reproduzindo Agora no topo**.

# Gerenciador de Plug-ins de Canal Virtual

## Introdução

O gerenciador de plug-ins de canal virtual foi projetado para implantar plug-ins em endpoints de cliente para aplicativos especificados. O gerenciador de plug-ins detecta aplicativos específicos em execução no VDA e solicita ao usuário que instale o plug-in no endpoint para obter a melhor experiência ao executar o aplicativo.

Os usuários podem optar por instalar o plug-in, ignorá-lo ou negar a instalação. O gerenciador de plug-ins oferece flexibilidade para gerenciar os plug-ins em todos os endpoints — gerenciados ou não gerenciados.

Por exemplo: o Microsoft Teams tem uma nova arquitetura (Otimização SlimCore), que exige que um plug-in seja instalado nos endpoints para que a otimização funcione. O gerenciador de plug-ins de canal virtual pode implantar os plug-ins em seus endpoints. Para obter mais informações, consulte nova solução VDI para Teams

## Requisitos do Sistema

A seguir estão os requisitos mínimos para o gerenciador de plug-ins de canal virtual.

- Agente de Área de Trabalho Virtual (VDA)
  - 2411
  - 2402 LTSR CU2
- DDC
  - Versão 121 da Nuvem
  - 2407 CR
  - 2402 LTSR CU1
- Aplicativo Citrix Workspace™ (Citrix Workspace App)
  - Aplicativo Citrix Workspace para Windows 2409

> **Nota:**
>
> Este recurso é atualmente aplicável a endpoints Windows.

### Aplicativos compatíveis

- Os aplicativos atualmente compatíveis estão listados abaixo:
  - Microsoft Teams - Consulte nova solução VDI para Teams

## Gerenciador de Plug-ins de Canal Virtual

### Implantação

1. Verifique se a política de redirecionamento do Microsoft Teams está ativada: Consulte política de redirecionamento do Microsoft Teams para obter mais detalhes.

   Esta política deve ser ativada independentemente do aplicativo que está sendo monitorado. No futuro, se mais aplicativos forem suportados e você quiser monitorar esses aplicativos em vez do Microsoft Teams, esta política ainda deverá ser ativada. Observe que esta política é ativada por padrão.

2. A política do gerenciador de plug-ins de canal virtual deve ser ativada: Consulte configurações da política do gerenciador de plug-ins de canal virtual para obter instruções detalhadas sobre como ativar a política.

   Esta política está disponível nas Configurações de Política Multimídia no Citrix Studio. A ativação da política permite especificar o nome do aplicativo a ser monitorado, por exemplo, “Microsoft Teams”. Esta política é desativada por padrão.

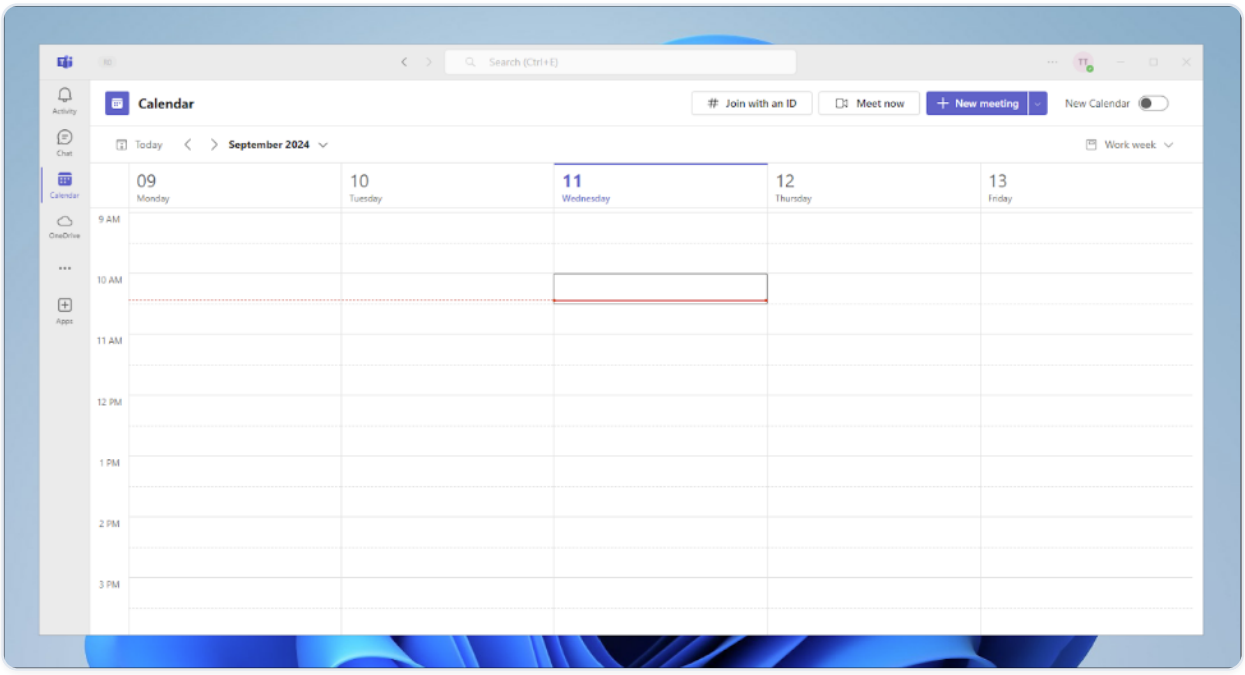
3. O aplicativo Citrix Workspace™ deve ser instalado no modo de sistema.

**Observação:**

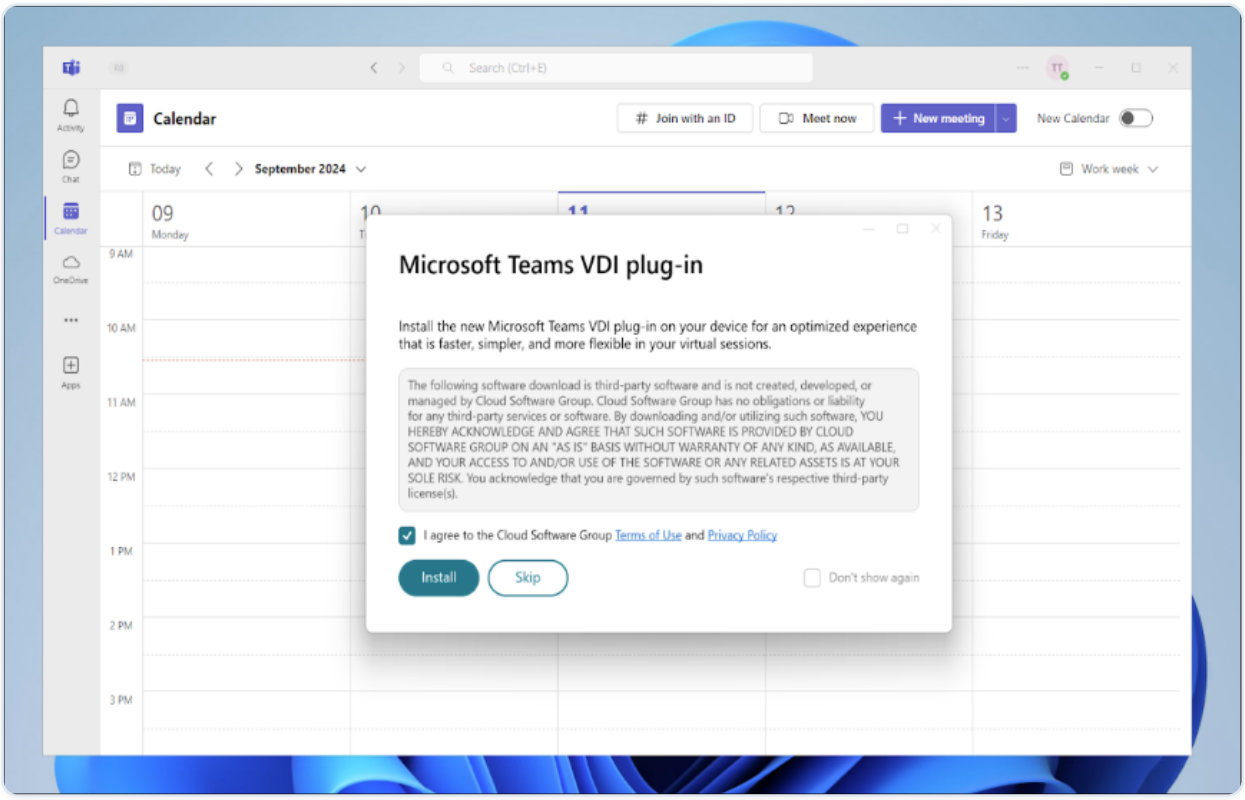
Os plug-ins são baixados para o endpoint a partir da CDN de terceiros. Por exemplo, se você selecionar o Microsoft Teams, o plug-in será baixado da CDN da Microsoft. Portanto, o endpoint deve ter acesso à CDN de terceiros. Caso contrário, a instalação do plug-in falhará.

### Procedimento

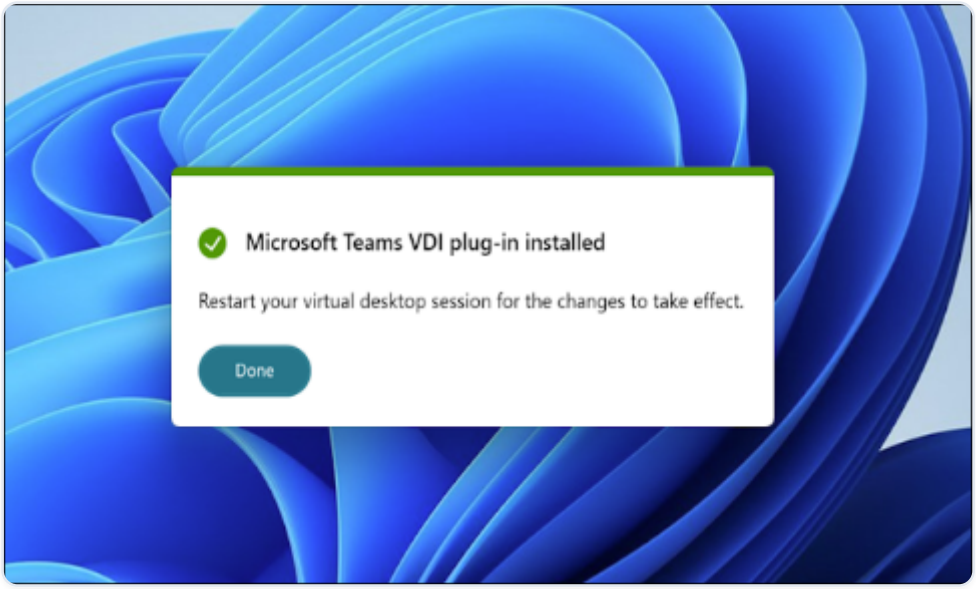
1. O usuário inicia o aplicativo na sessão Citrix. Por exemplo, Microsoft Teams.




2. O usuário recebe um pop-up para instalar o plug-in VDI do Teams no endpoint para uma melhor experiência. O pop-up aparece acima da sessão e não dentro da sessão, pois o plug-in será instalado no endpoint.




3. O usuário clica no botão de instalação e o plug-in é instalado. Os usuários precisam reiniciar a sessão da área de trabalho virtual para que as alterações entrem em vigor.




## Problemas Conhecidos e Limitações

- No VDA 2407, a seguinte configuração de registro precisa ser definida como 1 no VDA, além da política, para que o recurso seja ativado. Essa configuração de registro é automaticamente permitida e não precisa ser configurada a partir do VDA 2411.

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

Name: EnableAppDetector Type: DWORD`

- Mais limitações a serem adicionadas

# Otimização do SDK de Comunicações Unificadas

## Introdução

O Citrix Virtual Apps and Desktops permite que você entregue aplicativos aos seus usuários em uma ampla variedade de dispositivos de endpoint. Muitos desses aplicativos incluem recursos de comunicação em tempo real (RTC), como conferência de áudio e vídeo. No entanto, desafios podem surgir ao entregar esses aplicativos em um ambiente virtualizado. Métodos de entrega tradicionais roteiam fluxos de mídia (áudio/vídeo) do dispositivo cliente para o servidor VDI no data center antes de enviá-los de volta ao endpoint. Esse "hairpinning" introduz tráfego e sobrecarga de processamento desnecessários no servidor, especialmente para chamadas de áudio e vídeo que consomem muita largura de banda.

O Citrix Unified Communications SDK (UCSDK) é uma tecnologia que permite que fornecedores de tecnologia otimizem esses aplicativos RTC para uso em ambientes Citrix. Quando um aplicativo é otimizado, ele pode fornecer uma experiência de usuário que corresponde ou até excede a do aplicativo em execução em um desktop local. No mundo de hoje, a comunicação em tempo real contínua é essencial para a produtividade e colaboração. Ao usar aplicativos em um ambiente virtual, é crucial que chamadas de áudio e vídeo, compartilhamento de tela e outros recursos de comunicação funcionem tão suavemente quanto funcionariam em um desktop local. Aplicativos otimizados oferecem essa experiência.

Esta documentação do produto detalha tudo o que é necessário para que os clientes Citrix aprendam e implementem aplicativos otimizados com o UCSDK.

## Como funciona

A Citrix oferece um método de entrega otimizado para aplicativos de comunicação em tempo real dentro de VDIs. Essa abordagem aproveita o SDK de Comunicações Unificadas (UCSDK) para dividir o aplicativo virtualizado em duas partes:

- **Interface do Usuário (UI):** A interface do usuário permanece dentro do host virtual, exibida de forma contínua dentro do desktop virtual ou da janela do aplicativo.
- **Mecanismo de Mídia:** As tarefas de processamento de mídia (codificação/decodificação de áudio e vídeo) são descarregadas para o dispositivo local do usuário. Isso minimiza a carga do servidor e otimiza o uso da rede.

Normalmente, a Citrix oferece o UCSDK a fornecedores de tecnologia no espaço de comunicações em tempo real e trabalha com eles para integrar o UCSDK nesses aplicativos. Uma vez integrado, qualquer cliente Citrix que use um aplicativo otimizado com UCSDK terá uma experiência aprimorada. O Citrix UCSDK também pode ser consumido por clientes Citrix em casos onde um aplicativo interno personalizado está sendo desenvolvido. Na maioria dos casos, no entanto, os clientes não precisam consumir e desenvolver com o UCSDK – eles apenas precisam configurar o ambiente Citrix e o aplicativo para alcançar uma experiência otimizada.

> **Observação:**
>
> Referências ao Citrix WebRTC SDK (ou) a um aplicativo otimizado HDX™ indicam integração com o Citrix UCSDK e podem ser usadas de forma intercambiável.

## Principais Benefícios

Ao usar aplicativos otimizados com o Citrix UCSDK, você pode esperar:

- Desempenho aprimorado do processamento de mídia, descarregando a codificação/decodificação de mídia intensiva em processador do Citrix Virtual Delivery Agent (VDA) para o endpoint do cliente, aumentando a capacidade de resposta geral para os usuários finais.
- Uso reduzido de CPU e largura de banda no Citrix VDA, permitindo que a TI suporte mais usuários simultâneos por host e que as empresas escalem as implantações de desktop virtual Citrix de forma econômica.
- Menor custo total de propriedade para as empresas, pois os endpoints otimizados estendem a vida útil dos desktops virtuais legados e reduzem as necessidades de infraestrutura de host, diminuindo assim os gastos de capital e os custos operacionais ao longo do tempo.
- Suporte para plataformas de endpoint Windows, Mac, Linux, ChromeOS e HTML5.

## Casos de Uso

O UCSDK foi construído especificamente para otimizar aplicativos de comunicação em tempo real que aderem ao padrão WebRTC. Aqui estão os principais cenários e os tipos de aplicativos baseados em WebRTC que podem / já usam o UCSDK.

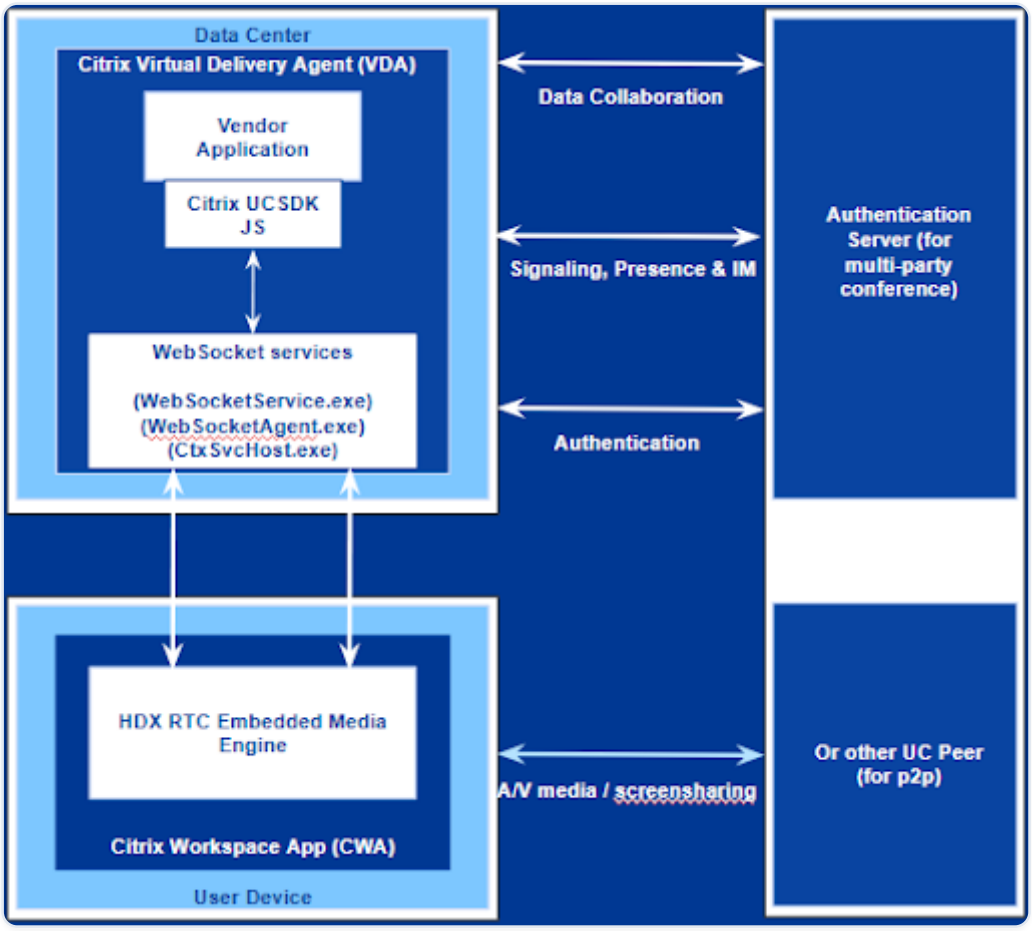
- **Contact Center como Serviço (CCaaS) / Plataformas de Contact Center na Nuvem:** Gerenciam principalmente as interações com os clientes em vários canais, otimizando os fluxos de trabalho dos agentes.

    - Exemplos: Amazon Connect, Twilio, Avaya Experience Platform, Talkdesk, Content Guru

- **Comunicações Unificadas como Serviço (UCaaS) / Comunicações Empresariais na Nuvem:** Integram voz, vídeo, mensagens de equipe e presença para uma comunicação empresarial abrangente.
    - Exemplos: Ring Central, 8x8, Intermedia, Alcatel-Lucent Rainbow
- **Plataforma de Comunicações como Serviço (CPaaS):** Fornecem APIs para incorporar recursos de comunicação em tempo real diretamente em aplicativos personalizados.
    - Exemplos: Twilio, Ribbon Communications
- **Videoconferência e Colaboração Empresarial:** Plataformas dedicadas para reuniões de vídeo de alta qualidade, conferências e recursos avançados de colaboração.
    - Exemplo: Pexip
- **Comunicações para Negociação Financeira:** Projetadas para as necessidades de comunicação exclusivas, de alto desempenho e em conformidade dos mercados financeiros.
    - Exemplo: IPC Unigy
- **Plataformas de Aprendizagem e Treinamento Virtual:** Projetadas para experiências interativas e de alta qualidade em salas de aula e treinamentos virtuais.
    - Exemplo: Vitero

A base WebRTC subjacente do Citrix UCSDK significa que suas capacidades de otimização podem se estender a quaisquer aplicativos de comunicação baseados em WebRTC. Isso abre a porta para otimizar uma ampla gama de aplicativos que utilizam WebRTC para interações em tempo real, mesmo que não estejam atualmente listados como otimizados com o UCSDK. Incentivamos os clientes a entrar em contato com a Citrix com quaisquer casos de uso ou aplicativos que desejam ver otimizados.

## Arquitetura do UCSDK




- Aplicativo do fornecedor: Pode ser qualquer aplicativo de comunicação em tempo real de terceiros, baseado em desktop ou navegador, que tenha integrado o UCSDK.
- UCSDK JS: O UCSDK JS fornece as APIs que os aplicativos do fornecedor utilizam para descarregar o áudio/vídeo para o endpoint.
- HdxRtcEngine: Este é o mecanismo de mídia WebRTC incorporado no Citrix Workspace App que processa e lida com a chamada de áudio/vídeo descarregada.

Uma vez que o SDK é carregado e usado, o processo `HdxRtcEngine.exe` é iniciado no endpoint do cliente se o redirecionamento for bem-sucedido. Uma vez que `HdxRtcEngine.exe` é iniciado no endpoint do cliente, quaisquer dados de sinalização e payload fluem do Citrix VDA para o endpoint do cliente, chegam à nuvem, retornam ao endpoint do cliente e são então encaminhados para o VDA. Por exemplo, um ciclo completo de fluxo poderia ser:

`Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App`

## Requisitos do Sistema

Os requisitos do sistema indicam as várias versões dos componentes Citrix necessários com a versão mais recente do UCSDK - 5.0.0. Para detalhes de compatibilidade para versões mais antigas do SDK e requisitos de recursos específicos, consulte a tabela Matriz de Versões e Recursos abaixo.

> **Observação:**
>
> Para que os clientes usem qualquer recurso adicionado ao UCSDK – certifique-se de que o aplicativo do fornecedor integrou a versão apropriada do UCSDK e ativou o recurso, e use as versões apropriadas de VDA e CWA em seu ambiente.

## Versões Totalmente Compatíveis

As versões totalmente compatíveis indicam que, ao usar essas versões dos componentes Citrix juntamente com a versão mais recente do UCSDK, os clientes podem aproveitar todos os recursos disponíveis. Para a versão mais recente atual do UCSDK – 5.0.0, as versões totalmente compatíveis dos componentes Citrix são as seguintes:

- **Citrix Virtual Apps e Desktops:** 2603
- **Citrix Workspace App Windows:** 2603
- **Citrix Workspace App Mac:** A ser lançado
- **Citrix Workspace App Linux:** 2603
- **Citrix Workspace App ChromeOS/HTML5:** A ser lançado

> **Observação:**
>
> A otimização do UCSDK é suportada em todas as plataformas de endpoint: Windows, Mac, Linux, ChromeOS e HTML5. Se a lista acima mostrar “A ser lançado” para uma plataforma de endpoint específica, isso significa simplesmente que uma versão totalmente compatível com os recursos mais recentes do UCSDK ainda não foi lançada. Assim, os clientes ainda podem usar versões mais antigas do aplicativo Citrix Workspace para continuar usando os recursos existentes, mesmo com o UCSDK mais recente.

## Configuração

A funcionalidade dos recursos do UCSDK depende de três fatores: a versão do UCSDK que o fornecedor integrou e os recursos que o fornecedor habilitou, o Citrix Virtual Apps and Desktops e a versão do aplicativo Citrix Workspace em uso.

No lado da Citrix, certifique-se de que o seguinte esteja configurado para que o aplicativo otimizado possa ser otimizado:

1. Certifique-se de que a política de redirecionamento do Microsoft Teams esteja ativada. Consulte Configurações de Política Multimídia para obter mais informações. Observe que esta política está ATIVADA por padrão.
2. Aplicativos de terceiros baseados em Electron ou navegador que utilizam o SDK `CitrixWebrtc.js` não são suportados por padrão. O `CtxHdxWebSocketService` (`WebSocketService.exe`) não permitirá conexões de aplicativos que não estejam na lista de permissões. O nome do executável binário do aplicativo desejado deve ser adicionado a uma chave de registro de lista de permissões.

> **Observação:**
>
> A partir do CVAD 2603, a otimização para aplicativos que usam o Citrix Unified Communications SDK (UCSDK) não depende mais da política de "redirecionamento do Microsoft Teams". Os administradores agora podem desabilitar a otimização do Microsoft Teams sem afetar outros aplicativos integrados ao UCSDK. Observe que, para usar essa separação, o aplicativo do fornecedor deve utilizar o método Bootstrap (introduzido pela primeira vez no UCSDK 4.0) juntamente com o CVAD 2603. Para mais detalhes, consulte Otimização Desacoplada do UCSDK e HDX Microsoft Teams

### No VDA

- Crie um Caminho de Chave: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- Nome da Chave: `ProcessWhitelist`
- Tipo: `MULTISZ`
- Valor da Chave: `Mytestapp.exe`

Se você tiver vários aplicativos, digite cada aplicativo em uma nova linha. Não copie e cole de um arquivo de texto nem insira vírgulas. Certifique-se de que o nome fornecido corresponda ao nome do executável do aplicativo. Este valor de registro não diferencia maiúsculas de minúsculas.

Se o aplicativo for acessado por meio de um navegador em vez de um aplicativo de desktop completo, então você precisa permitir, por exemplo, `chrome.exe` no valor do registro.

Uma vez que o registro acima esteja configurado com sucesso, reinicie o VDA ou reinicie `CtxHdxWebSocketService` para finalizar a configuração da Lista de Permissões.

#### No Cliente

Nenhuma configuração é necessária. Basta instalar o aplicativo Citrix Workspace.

Cada fornecedor pode ter um nome de aplicativo muito específico. Portanto, consulte a documentação do fornecedor vinculada na seção Suporte ao Fornecedor Atual para determinar qual nome de aplicativo deve ser permitido no WebSocketService.

## Referência de Recursos

### Tempos de Conexão de Chamada Aprimorados com Smart Sync

Introduzido no UCSDK 5.0.0, o recurso Smart Sync acelera os tempos de conexão de chamadas ao otimizar a comunicação entre o VDA e o endpoint do cliente. Este aprimoramento oferece configurações de chamadas mais rápidas em geral, proporcionando as melhorias de desempenho mais significativas para ambientes de rede de alta latência.

A Citrix recomenda que os clientes entrem em contato com seus fornecedores de aplicativos para atualizar para o UCSDK 5.0.0 para aproveitar este recurso.

> **Observação:**

> Este recurso depende apenas do UCSDK 5.0.0 e do aplicativo Citrix Workspace. Consulte a Matriz de Versões e Recursos para as versões exatas do cliente. Não há dependência de versão do VDA, então VDAs mais antigos e suportados ainda podem ser usados.

## Matriz de Versões e Recursos

Como as atualizações de versão ocorrem frequentemente, consulte as páginas de ciclo de vida do produto Citrix Virtual Apps and Desktops e Citrix Workspace app para garantir que uma versão específica seja suportada. Para muitos dos recursos mais antigos, as versões mencionadas na tabela são as últimas versões de Lançamento Atual (CR) suportadas no momento da redação deste documento.

| RECURSO | VERSÃO DO UCSDK | VDA | CWA WINDOWS | CWA MAC | CWA LINUX | CWA CHROME OS/ HTML5 |
|---|---|---|---|---|---|---|
| Áudio / Vídeo (p2p e conferência) | 3.1.0 | 2203 LTSR Latest CU / 2311 CR | 2402 LTSR Latest CU / 2311 CR | 2311 | 2311 | 2312 |
| Compartilhamento de tela | 3.1.0 | 2203 LTSR Latest CU / 2311 CR | 2402 LTSR Latest CU / 2311 CR | 2311 | 2311 | 2312 |
| DTMF | 3.1.0 | 2203 LTSR Latest CU / 2311 CR | 2402 LTSR Latest CU / 2311 CR | 2311 | 2311 | 2312 |
| Suporte a Servidor Proxy | 3.1.0 | 2203 LTSR CU Mais Recente / 2311 CR | 2402 LTSR CU Mais Recente / 2311 CR | 2311 | 2311 | 2312 |
| Compartilhamento de apps | 3.1.0 | 2203 LTSR CU Mais Recente / 2311 CR | 2402 LTSR CU Mais Recente / 2311 CR | 2311 | 2311 | N/A |
| e911 Dinâmico | 3.1.0 | 2203 LTSR Latest CU / 2311 CR | 2402 LTSR Latest CU / 2311 CR | 2311 | 2311 | 2312 |
| Multi Janela | 3.1.0 | 2203 LTSR Latest | 2402 LTSR Latest | 2311 | 2311 | 2312 |

| RECURSO | VERSÃO DO UCSDK | VDA | CWA WINDOWS | CWA MAC | CWA LINUX | CWA CHROME OS/ HTML5 |
|---|---|---|---|---|---|---|
| | | CU / 2311 CR | CU / 2311 CR | | | |
| Suporte ao Plano Unificado SDP | 3.1.0 | 2203 LTSR Latest CU / 2311 CR | 2402 LTSR CU Mais Recente / 2311 CR | 2311 | 2311 | 2312 |
| Resolução de stream / Simulcast | 3.1.0 | 2203 LTSR CU Mais Recente / 2311 CR | 2402 LTSR CU Mais Recente / 2311 CR | 2311 | 2311 | 2312 |
| Áudio Remoto (com Loop) | 3.1.0 | 2203 LTSR CU Mais Recente / 2311 CR | 2402 LTSR CU Mais Recente / 2311 CR | 2311 | 2311 | 2405 |
| UCSDK baseado em navegador (suporte a Bootstrap) | 4.0.2 | 2407 CR | 2402 LTSR CU mais recente / 2311 CR | 2311 | 2311 | 2312 |
| API Web HID | 4.0.2 | 2203 LTSR CU mais recente / 2311 CR | 2409.10 | 2411 | 2411 | 2505 |
| Web Audio API | 4.0.2 | 2203 LTSR Latest | 2405 | 2405 | 2405 | N/A |

| RECURSO | VERSÃO DO UCSDK | VDA | CWA WINDOWS | CWA MAC | CWA LINUX | CWA CHROME OS/ HTML5 |
|---|---|---|---|---|---|---|
| | | CU / 2311 CR | | | | |
| Reiniciar ICE | 4.1.0 | 2203 LTSR Latest CU / 2311 CR | 2503.2 | 2503 | 2503 | 2502.10 |
| Gravação de Tela (Prévia)[1] | 4.1.0 | 2503 | 2503.2 | N/A | N/A | N/A |
| Smart Sync | 5.0.0 | 2203 LTSR CU mais recente / 2311 CR | 2603 | N/A | 2604 | N/A |

**Observação:**

Introduzimos uma nova política para gravação de tela, então você precisa da versão 2503 do delivery controller™, que vem com o CVAD 2503.

## Suporte Atual do Fornecedor

Vários fornecedores terceirizados integraram o SDK de Comunicações Unificadas em seus produtos. A lista atual de fornecedores e sua documentação de suporte está listada abaixo:

| FORNECEDOR | DOCUMENTAÇÃO |
|---|---|
| Sprinklr | Descarregamento de Mídia Citrix para Chamadas de Voz - Sprinklr |
| Amazon Connect | Otimizar áudio do Amazon Connect para desktops em nuvem Citrix |

| FORNECEDOR | DOCUMENTAÇÃO |
| --- | --- |
| Ring Central | Usando RingCentral em um ambiente Citrix VDI |
| Five9 | Five9 WebRTC em ambientes Citrix |
| Twilio | Twilio Flex em Citrix VDI |
| Avaya | Solução VDI de Nuvem Pública da Plataforma Avaya Experience para Citrix |
| 8x8 | Integração Citrix VDI com 8x8 Work para Desktop e Web |
| Content Guru | Integração Content Guru Citrix |
| Ribbon Communications | SDK WebRTC da Ribbon Communications para Citrix |
| Intermedia | Instalando o Intermedia Unite em Citrix Virtual Apps and Desktops |
| Alcatel-Lucent Rainbow | Otimização Citrix para o Aplicativo de Desktop Rainbow |
| Talkdesk | Talkdesk Agent Workspace VDI Connect |
| IPC | IPC Unigy Soft Client Citrix VDI |
| Vitero | Vitero Inspire para Citrix VDI |
| Pexip | Implantação do aplicativo de desktop Connect em Citrix Pexip Infinity Docs |
| Zoom Web App | Configurar o redirecionamento WebRTC para o aplicativo Web Zoom |

## Solução de problemas

Para obter informações sobre solução de problemas, consulte Orientações para Solução de Problemas de Aplicativos Otimizados com o SDK de Comunicações Unificadas da Citrix.

# Problemas Conhecidos e Limitações

Esta seção documentará os problemas e limitações conhecidos atuais à medida que forem reconhecidos.

# Redirecionamento geral de conteúdo

O redirecionamento de conteúdo permite controlar se os usuários acessam informações usando aplicativos publicados em servidores ou usando aplicativos executados localmente em dispositivos de usuário.

Redirecionamento de pasta do cliente(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/client-folder-redirection.html)

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host.

- Quando você habilita apenas o mapeamento de unidade do cliente no servidor, os volumes completos do lado do cliente são automaticamente mapeados para as sessões como links de Convenção Universal de Nomenclatura (UNC).
- Quando você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo de desktop Windows, a parte do volume local especificada pelo usuário é redirecionada.

Redirecionamento do host para o cliente(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/host-to-client-redirection.html)

Considere usar o redirecionamento do host para o cliente para casos de uso incomuns específicos. Normalmente, outras formas de redirecionamento de conteúdo podem ser melhores. Oferecemos suporte a esse tipo de redirecionamento apenas em VDAs de SO de múltiplas sessões e não em VDAs de SO de sessão única.

Acesso a aplicativos locais e redirecionamento de URL(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/laa-url-redirect.html)

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de desktop hospedado. Isso é feito sem a necessidade de alternar de um computador para outro.

A tecnologia HDX™ oferece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde ele é inadequado.

# Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Se você habilitar apenas o mapeamento de unidade do cliente no servidor, os volumes completos do lado do cliente serão automaticamente mapeados como links de Convenção Universal de Nomenclatura (UNC) para as sessões. Quando você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo do usuário, a parte do volume local especificada pelo usuário é redirecionada.

Apenas as pastas especificadas pelo usuário aparecem como links UNC dentro das sessões. Ou seja, em vez do sistema de arquivos completo no dispositivo do usuário. Se você desabilitar os links UNC através do registro, as pastas do cliente aparecerão como unidades mapeadas dentro da sessão.

O redirecionamento de pasta do cliente é suportado apenas em máquinas Windows Single-session OS.

O redirecionamento de pasta do cliente para uma unidade USB externa não é salvo ao desconectar e reconectar o dispositivo.

Habilite o redirecionamento de pasta do cliente no servidor. Em seguida, no dispositivo cliente, especifique quais pastas redirecionar. O aplicativo que você usa para especificar as opções de pasta do cliente está incluído no aplicativo Citrix Workspace™ fornecido com esta versão.

**Requisitos:**

Para servidores:

- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter
- Windows Server 2012 R2, edições Standard e Datacenter

Para clientes:

- Windows 10, edições de 32 bits e 64 bits (versão mínima 1607)
- Windows 8.1, edições de 32 bits e 64 bits (incluindo a edição Embedded)
- Windows 7, edições de 32 bits e 64 bits (incluindo a edição Embedded)

Para habilitar o redirecionamento de pasta do cliente no servidor, consulte Redirecionamento de pasta do cliente na lista de recursos gerenciados através do registro.

No dispositivo do usuário, especifique quais pastas redirecionar:

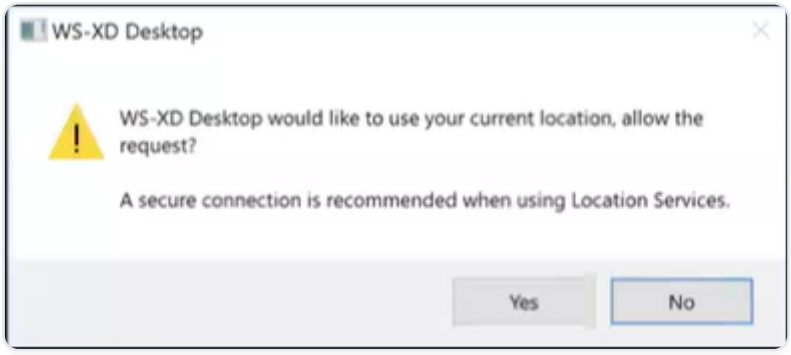
1. Certifique-se de que a versão mais recente do aplicativo Citrix Workspace esteja instalada.
2. No diretório de instalação do aplicativo Citrix Workspace, inicie CtxCFRUI.exe.
3. Escolha o botão de opção **Personalizado** e adicione, edite ou remova pastas.
4. Desconecte e reconecte suas sessões para que a configuração entre em vigor.

# Redirecionamento de localização do cliente

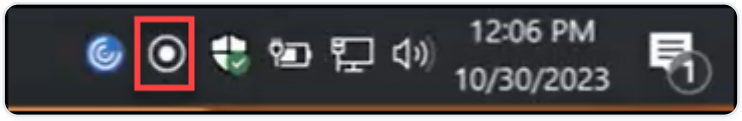
O redirecionamento de localização do cliente, quando ativado, permite que aplicativos e sessões de desktop hospedados em VDA acessem perfeitamente a localização atual do cliente. Em um sistema operacional multi-sessão (TS VDA ou Multi-Session WS VDA), cada sessão tem sua própria localização exclusiva fornecida pelo cliente conectado. Usando esse recurso, os aplicativos no VDA que dependem da localização têm a localização precisa do cliente.

Para obter mais informações, consulte a documentação Microsoft.

Depois que o redirecionamento de localização do cliente é ativado e o acesso à localização é permitido tanto no lado do servidor quanto no lado do cliente, ao iniciar um aplicativo ou desktop que acessa a localização, o cliente solicita que você compartilhe sua localização atual com a seguinte caixa de diálogo:




Ao ativar o redirecionamento de localização do cliente, o seguinte ícone aparece na barra de tarefas do cliente se/quando o aplicativo ou desktop hospedado no VDA consulta informações de localização atual.




## Requisitos do sistema

Para servidores:

- VDA de SO de sessão única (Win10/11) ou multi-sessão (Win 11 22H2 e Server 2022 23H2 ou posterior)
- Aplicativo Citrix Workspace™ para Windows, iOS ou Android

### Configuração

O redirecionamento de localização do cliente deve ser ativado usando a política Citrix® para que o recurso funcione. O redirecionamento de localização do cliente é desativado por padrão.

Para ativar o redirecionamento de localização do cliente, conclua as seguintes etapas:

No lado do VDA e Cliente Windows:

1. Em **Configurações > Privacidade > Localização**, ative as seguintes opções:
    - **Permitir acesso à localização neste dispositivo**
    - **Permitir que aplicativos acessem sua localização**
    - **Permitir que aplicativos de desktop acessem sua localização**
2. Para SO de múltiplas sessões, ative a configuração **Substituição de Localização**.

No lado do Controller/DDC:

Ative a política **Studio > Políticas > Localização > Configurações > Permitir que o aplicativo use a localização física do dispositivo cliente**. Para obter mais informações, consulte Configurações de política de sensores do cliente.

## Redirecionamento de conteúdo bidirecional

O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS em navegadores da web, ou incorporadas em aplicativos, sejam encaminhadas entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Uma URL inserida em um navegador em execução na sessão Citrix pode ser aberta usando o navegador padrão do cliente. Por outro lado, uma URL inserida em um navegador em execução no cliente pode ser aberta em uma sessão Citrix, seja com um aplicativo ou desktop publicado. Alguns casos de uso comuns para o redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da web em casos em que o navegador inicial não tem acesso à rede para a origem.
- Redirecionamento de URLs da web por motivos de compatibilidade do navegador e segurança.

- Redirecionamento de URLs da web incorporadas em aplicativos quando não se deseja executar um navegador da web na sessão Citrix ou no cliente.

## Requisitos do sistema

- VDAs de SO de sessão única ou multissessão
- Aplicativo Citrix Workspace™ para Windows 2311 ou superior
- Aplicativo Citrix Workspace™ para Linux 2503 ou superior
- Aplicativo Citrix Workspace™ para Mac 2607 ou superior

Navegadores:

- Google Chrome com a Extensão de Redirecionamento de Navegador Citrix
  - Extensão do Google Chrome
- Microsoft Edge com a Extensão de Redirecionamento de Navegador Citrix
  - Extensão do Microsoft Edge

## Configuração

A partir da versão 2311 do Citrix Virtual Apps and Desktops™, o redirecionamento de conteúdo bidirecional é configurado apenas através do Citrix Studio. Versões anteriores tinham configurações de política configuradas tanto no endpoint do cliente quanto no Studio. O redirecionamento de conteúdo bidirecional é desabilitado por padrão.

Para configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações da **política ICA**.

Para que o redirecionamento do navegador funcione, as extensões do navegador devem ser registradas no navegador de origem (de onde a URL é redirecionada) usando os comandos mostrados. Execute os comandos conforme necessário no VDA e no cliente, com base no navegador em uso.

| NAVEGADOR | VDA | CLIENTE |
| --- | --- | --- |
| Google Chrome | "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome | "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome |

| NAVEGADOR | VDA | CLIENTE |
|---|---|---|
| Microsoft Edge | "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge | "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge |
| Todos os Navegadores Disponíveis | "%ProgramFiles(x86)%\Citrix\HDX\binários\vdaredirector.exe" /regall | "%ProgramFiles(x86)%\Citrix\ICA Cliente\redirector.exe" /regall |

Para cancelar o registro de uma extensão de navegador:

| NAVEGADOR | VDA | CLIENTE |
|---|---|---|
| Google Chrome | "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome | "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome |
| Microsoft Edge | "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge | "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge |
| Todos os Navegadores Disponíveis | "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall | "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall |

**Nota:**

- Execute esses comandos em uma janela do Prompt de Comando (CMD) com privilégios de administrador.
- O comando de registro faz com que os navegadores Chrome e Edge solicitem aos usuários que habilitem a Extensão de Redirecionamento de Navegador Citrix durante o primeiro lançamento.

- O comando de registro também vincula a Extensão de Redirecionamento de Navegador ao host de mensagens nativas, o que permite que a extensão se comunique com o código nativo. Sem isso, o navegador bloqueia a comunicação.
- Você também pode instalar a extensão do navegador manualmente na Google Chrome Web Store. Para usar a Extensão de Redirecionamento de Navegador da loja de Complementos do Microsoft Edge, você precisa da versão 2503 ou posterior do Virtual Delivery Agent (VDA). Para versões mais antigas do VDA, instale a extensão da Google Chrome Web Store dentro do seu navegador Microsoft Edge (consulte Adicionar uma extensão ao Microsoft Edge da Chrome Web Store).
- As versões do aplicativo Citrix Workspace listadas nos requisitos do sistema são as versões mínimas necessárias para oferecer suporte ao redirecionamento de conteúdo bidirecional e ao redirecionamento OAuth.
- Para Mac: devido aos requisitos de segurança do macOS para aplicativos autenticados, os esquemas de URL de retorno de chamada OAuth personalizados devem ser pré-registrados com a Citrix e não podem ser alterados dinamicamente após a instalação. Apenas `citrix-oauth-redir` é suportado por padrão. Entre em contato com a equipe de produto da Citrix para registrar seu esquema de URL.

## Redirecionamento curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de curingas ao definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

## Redirecionamento de protocolo personalizado do VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao redirecionamento de protocolos personalizados do Citrix VDA para o cliente. Protocolos diferentes de HTTP ou HTTPS são suportados. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Web Studio, defina o protocolo personalizado em **Redirecionamento de conteúdo bidirecional**.

**Observação:**

- Você deve ter privilégios de administrador para executar esses comandos.
- O cliente deve ter um aplicativo registrado para manipular o protocolo. Caso contrário, a URL redireciona para o cliente e falha ao iniciar.
- URLs de protocolo personalizado que você insere ou inicia nos navegadores Chrome e Edge não são suportadas e não são redirecionadas.
- Os seguintes protocolos não são suportados: `rtsp://, rtspu://, pnm://, mms://`.

### Outras considerações

- Os requisitos e configurações do navegador são aplicáveis apenas ao navegador que inicia o redirecionamento. O navegador de destino, onde a URL é aberta após o redirecionamento ser bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, uma configuração de navegador suportada é necessária apenas no VDA. Inversamente, ao redirecionar URLs do cliente para um VDA, uma configuração de navegador suportada é necessária apenas no cliente. As URLs redirecionadas são entregues ao navegador padrão configurado na máquina de destino, seja o cliente ou o VDA, dependendo da direção. Não é necessário usar o mesmo tipo de navegador no VDA e no cliente.
- Verifique se as regras de redirecionamento não resultam em uma configuração em loop. Por exemplo, uma política de VDA é definida para redirecionar `https://www.citrix.com`, e a política do cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Encurtadores de URL não são suportados.
- O redirecionamento de cliente para VDA requer que o cliente Windows seja instalado com direitos de administrador.
- Se o navegador de destino já estiver aberto, a URL redirecionada será aberta em uma nova guia. Caso contrário, a URL será aberta em uma nova janela do navegador.
- O redirecionamento bidirecional de conteúdo não funciona quando o Acesso a Aplicativos Locais (LAA) está ativado.

## Redirecionamento do host para o cliente

O redirecionamento do host para o cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix®, sejam abertas usando o aplicativo correspondente no dispositivo de endpoint do usuário. Alguns casos de uso comuns para o redirecionamento do host para o cliente incluem:

- Redirecionamento de sites em casos em que o servidor Citrix não tem acesso à Internet ou à rede para a origem.
- Redirecionamento de sites quando a execução de um navegador da web dentro da sessão Citrix não é desejada por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos em casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento do host para o cliente não se destina a URLs que você acessa em uma página da web ou digita na barra de endereços do navegador da web em execução na sessão Citrix. Para redirecionamento de URLs em navegadores da web, consulte Redirecionamento bidirecional de URL ou Redirecionamento de conteúdo do navegador.

## Requisitos do sistema

- VDA de SO multissessão
- Clientes compatíveis:
  - Citrix Workspace™ app para Windows
  - Aplicativo Citrix Workspace para Mac
  - Aplicativo Citrix Workspace para Linux
  - Aplicativo Citrix Workspace para HTML5
  - Aplicativo Citrix Workspace para Chrome

O dispositivo cliente deve ter um aplicativo instalado e configurado para lidar com o redirecionamento dos tipos de URL.

## Configuração

Use a política Citrix Redirecionamento do host para o cliente para habilitar esta funcionalidade. **O redirecionamento do host para o cliente** está desabilitado por padrão. Depois de habilitar a política de redirecionamento do host para o cliente, o aplicativo Citrix Launcher se registra no servidor Windows para garantir que ele possa interceptar URLs e enviá-las para o dispositivo cliente.

Em seguida, você deve configurar a Política de Grupo do Windows para usar o Citrix Launcher como o aplicativo padrão para os tipos de URL necessários. No VDA do servidor Citrix, crie o arquivo ServerFTAdefaultPolicy.xml e insira o seguinte código XML.

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

No console de gerenciamento de Política de Grupo, vá para **Configuração do computador > Modelos Administrativos > Componentes do Windows > Explorador de Arquivos > Definir um arquivo de configuração de associações padrão**, e salve seu arquivo ServerFTAdefaultPolicy.xml.

**Observação:**

Se um servidor Citrix não tiver as configurações da Política de Grupo, o Windows solicitará aos usuários que selecionem um aplicativo para abrir URLs.

Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM

- MMS

Para incluir tipos de URL padrão ou personalizados adicionais na lista para redirecionamento, crie uma nova linha **Association Identifier** no arquivo ServerFTAdefaultPolicy.xml referenciado anteriormente. Por exemplo:

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

Adicionar tipos de URL à lista também requer configuração do cliente. Crie a seguinte chave de registro e valores no cliente Windows.

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

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome do valor: ExtraURLProtocols
- Tipo de valor: REG_SZ
- Dados do valor: Especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade da URL. Por exemplo: `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL apenas para clientes Windows. Clientes que não possuem as configurações de registro acima rejeitam o redirecionamento de volta para a sessão Citrix. O

cliente deve ter um aplicativo instalado e configurado para manipular os tipos de URL especificados.

Para remover tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD
- Dados do valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm`, ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

`http`

`https`

`rtsp`

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, crie uma chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: ValidSites
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este curinga corresponde a um único nível de domínio, o que é consistente com as regras no RFC 6125. Por exemplo:

`www.exmaple.com`

`*.example.com`

> **Observação:**

> Não é possível usar a chave **ValidSites** com as chaves **DisableServerFTA** e **NoRedirectClasses**.

### Configuração padrão do navegador do VDA do servidor

A habilitação do redirecionamento do host para o cliente, conforme referenciado nesta seção, substitui qualquer configuração anterior do navegador padrão no VDA do servidor. Se um URL da web não for redirecionado, o Citrix Launcher passará o URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente. Para obter mais informações, consulte Configuração do navegador padrão do VDA do servidor na lista de recursos gerenciados por meio do registro.

## Acesso a Aplicativos Locais e redirecionamento de URL

### Introdução

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Com o Acesso a Aplicativos Locais, você pode:

- Acessar aplicativos instalados localmente em um laptop físico, PC ou outro dispositivo diretamente da área de trabalho virtual.
- Fornecer uma solução flexível de entrega de aplicativos. Se os usuários tiverem aplicativos locais que você não pode virtualizar ou que a TI não mantém, esses aplicativos ainda se comportarão como se estivessem instalados em uma área de trabalho virtual.
- Eliminar a latência de salto duplo quando os aplicativos são hospedados separadamente da área de trabalho virtual. Faça isso colocando um atalho para o aplicativo publicado no dispositivo Windows do usuário.
- Usar aplicativos como:
  - Software de videoconferência como o GoToMeeting.
  - Aplicativos especializados ou de nicho que ainda não foram virtualizados.
  - Aplicativos e periféricos que, de outra forma, transfeririam grandes quantidades de dados de um dispositivo de usuário para um servidor e de volta para o dispositivo de usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops™, as sessões de área de trabalho hospedada usam o redirecionamento de URL para iniciar aplicativos de Acesso a Aplicativos Locais. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de bloqueio de URL do navegador) selecionando links incorporados em um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueio, o URL será aberto novamente na sessão da área de trabalho.

O redirecionamento de URL funciona apenas para sessões de área de trabalho, não para sessões de aplicativo. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo host-para-cliente, que é um tipo de redirecionamento FTA (Associação de Tipo de Arquivo) do servidor. Este FTA redireciona certos protocolos para o cliente, como HTTP, HTTPS, RTSP ou MMS. Por exemplo, se você abrir apenas links incorporados com HTTP, os links serão abertos diretamente com o aplicativo cliente. Não há suporte para lista de bloqueio ou lista de permissões de URL.

Quando o Acesso a Aplicativos Locais está ativado, os URLs exibidos aos usuários como links de aplicativos em execução localmente, de aplicativos hospedados pelo usuário ou como atalhos na área de trabalho são redirecionados de uma das seguintes maneiras:

- Do computador do usuário para a área de trabalho hospedada
- Do servidor Citrix Virtual Apps and Desktops para o computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento de conteúdo de sites específicos, configure a lista de permissões de URL e a lista de bloqueios de URL no Virtual Delivery Agent. Essas listas contêm chaves de registro de várias strings que especificam as configurações da política de redirecionamento de URL. Para obter mais informações, consulte as configurações da política de Acesso a Aplicativos Locais.

As URLs podem ser renderizadas no VDA com as seguintes exceções:

- Informações de Geo/Localidade — Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na Geo). Por exemplo, se o VDA for provisionado de um data center no Reino Unido e o cliente estiver se conectando da Índia, o usuário espera ver in.msn.com. Em vez disso, o usuário vê uk.msn.com.
- Conteúdo multimídia — Sites que contêm conteúdo de mídia rica, quando renderizados no dispositivo cliente, proporcionam aos usuários finais uma experiência nativa e também

economizam largura de banda, mesmo em redes de alta latência. Esse recurso redireciona sites com outros tipos de mídia, como Silverlight. Esse processo ocorre em um ambiente seguro. Ou seja, as URLs que o administrador aprova são executadas no cliente, enquanto o restante das URLs é redirecionado para o VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, ele deverá ter acesso ao arquivo para abri-lo. Portanto, você só pode abrir arquivos que residem em compartilhamentos de rede ou em unidades de cliente (usando o mapeamento de unidade de cliente) usando aplicativos locais. Por exemplo, ao abrir um arquivo PDF, se um leitor de PDF for um aplicativo local, o arquivo será aberto usando esse leitor de PDF. Como o aplicativo local pode acessar o arquivo diretamente, não há transferência de rede do arquivo via ICA® para abri-lo.

## Requisitos, considerações e limitações

Oferecemos suporte ao Acesso a Aplicativos Locais nos sistemas operacionais válidos para VDAs para Windows Multi-session OS e para VDAs para Windows Single-session OS. O Acesso a Aplicativos Locais requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são suportados:

- Edge, versão mais recente
- Firefox, versão mais recente e versão de suporte estendido
- Chrome, versão mais recente

Revise as seguintes considerações e limitações ao usar o Acesso a Aplicativos Locais e o redirecionamento de URL.

- O Acesso a Aplicativos Locais foi projetado para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o Acesso a Aplicativos Locais com um desktop virtual que é executado no modo de janela ou não cobre todos os monitores.
  - Vários monitores — Quando um monitor é maximizado, ele se torna o desktop padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo que os aplicativos subsequentes normalmente iniciem em outro monitor.
  - O recurso suporta um VDA. Não há integração com múltiplos VDAs simultâneos.
- Alguns aplicativos podem se comportar de forma inesperada, afetando os usuários:

- As letras das unidades podem confundir os usuários, como C: local em vez da unidade C: da área de trabalho virtual.
- As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
- Aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados no cliente.
- Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).
- Aplicativos locais aparecem com o tema do Windows da máquina local.
- Aplicativos em tela cheia não são suportados. Esses aplicativos incluem aplicativos que abrem em tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem a área de trabalho inteira.
- O Acesso a Aplicativos Locais copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e no menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
- Aplicativos que personalizam como a ordem das janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
- Atalhos não são suportados, incluindo Meu Computador, Lixeira, Painel de Controle, atalhos de Unidade de Rede e atalhos de pasta.
- Os seguintes tipos de arquivo e arquivos não são suportados: tipos de arquivo personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
- O agrupamento da barra de tarefas não é suportado para aplicativos hospedados no cliente ou VDA mistos de 32 bits e 64 bits. Ou seja, agrupar aplicativos locais de 32 bits com aplicativos VDA de 64 bits.
- Aplicativos não podem ser iniciados usando COM. Por exemplo, se você clicar em um documento do Office incorporado de dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local falhará.

- Cenários de salto duplo, onde um usuário está iniciando uma área de trabalho virtual de dentro de outra sessão de área de trabalho virtual, não são suportados.
- O redirecionamento de URL suporta apenas URLs explícitas (ou seja, URLs que aparecem na barra de endereços do navegador ou encontradas usando a navegação no navegador, dependendo do navegador).

- O redirecionamento de URL funciona apenas com sessões de desktop, não com sessões de aplicativo.
- A pasta de desktop local em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução localmente se comportam de acordo com as configurações da barra de tarefas estabelecidas para o desktop virtual. No entanto, os atalhos para aplicativos em execução localmente não são agrupados com instâncias em execução desses aplicativos. Eles também não são agrupados com instâncias em execução de aplicativos hospedados ou atalhos fixados para aplicativos hospedados. Os usuários podem fechar apenas janelas de aplicativos em execução localmente a partir da Barra de Tarefas. Embora os usuários possam fixar janelas de aplicativos locais na Barra de Tarefas e no menu Iniciar do desktop, os aplicativos podem não iniciar de forma consistente ao usar esses atalhos.
- Se você definir a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**, o redirecionamento de conteúdo do navegador não é suportado. Por padrão, o Acesso a Aplicativos Locais é proibido.

## Interação com o Windows

A interação do Acesso a Aplicativos Locais com o Windows inclui os seguintes comportamentos.

- Comportamento de atalho do Windows 8 e Windows Server 2012
  - Os aplicativos da Windows Store instalados no cliente não são enumerados como parte dos atalhos do Acesso a Aplicativos Locais.
  - Arquivos de imagem e vídeo são abertos por padrão usando aplicativos da Windows Store. No entanto, o Acesso a Aplicativos Locais enumera os aplicativos da Windows Store e abre atalhos com aplicativos de desktop.
- Programas Locais
  - Para o Windows 7, a pasta está disponível no menu Iniciar.
  - Para o Windows 8, Programas Locais está disponível apenas quando o usuário escolhe **Todos os Aplicativos** como uma categoria na tela Iniciar. Nem todas as subpastas são exibidas em Programas Locais.
- Recursos gráficos do Windows 8 para aplicativos
  - Os aplicativos de desktop são restritos à área de trabalho e são cobertos pela tela Iniciar e aplicativos estilo Windows 8.

  - Os aplicativos de Acesso a Aplicativos Locais não se comportam como aplicativos de desktop no modo de vários monitores. No modo de vários monitores, a tela Iniciar e a área de trabalho são exibidas em monitores diferentes.

- Windows 8 e Redirecionamento de URL de Acesso a Aplicativos Locais
  - Como o Internet Explorer do Windows 8 não tem complementos habilitados, use o Internet Explorer da área de trabalho para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desabilita os complementos por padrão. Para implementar o Redirecionamento de URL, desabilite a configuração aprimorada do Internet Explorer. Em seguida, redefina as opções do Internet Explorer e reinicie para garantir que os complementos estejam habilitados para usuários padrão.

## Configurar o Acesso a Aplicativos Locais e o redirecionamento de URL

Para usar o Acesso a Aplicativos Locais e o redirecionamento de URL com o aplicativo Citrix Workspace™:

- Instale o aplicativo Citrix Workspace na máquina cliente local. Você pode habilitar ambos os recursos durante a instalação do aplicativo Citrix Workspace ou pode habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo.
- Defina a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**. Você também pode configurar as configurações de política de lista de permissões e lista de bloqueios de URL para redirecionamento de URL. Para obter mais informações, consulte Configurações de política de Acesso a Aplicativos Locais.

### Habilitar o Acesso a Aplicativos Locais e o redirecionamento de URL

Para habilitar o Acesso a Aplicativos Locais para todos os aplicativos locais, siga estas etapas:

1. Faça login no Web Studio e clique em **Políticas** no painel esquerdo.
2. Na barra de ações, clique em **Criar Política**.
3. Na janela Criar Política, digite "Permitir Acesso a Aplicativos Locais" na caixa de pesquisa e clique em **Selecionar**.
4. Na janela Editar Configuração, selecione **Permitido**. Por padrão, a política **Permitir acesso a aplicativos locais** é proibida. Quando essa configuração é permitida, o VDA permite que o usuário final decida se os aplicativos publicados e os atalhos de Acesso a Aplicativos Locais são habilitados na sessão. (Quando essa configuração é proibida, tanto os aplicativos publicados quanto os atalhos de Acesso a Aplicativos Locais não funcionam para o VDA.)

Essa configuração de política se aplica a toda a máquina e à política de redirecionamento de URL.

5. Na janela Criar Política, digite "Lista de permissões de redirecionamento de URL" na caixa de pesquisa e clique em **Selecionar**. A lista de permissões de redirecionamento de URL especifica URLs a serem abertas no navegador padrão da sessão remota.
6. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
7. Na janela Criar Política, digite "Lista de bloqueios de redirecionamento de URL" na caixa de pesquisa e clique em **Selecionar**. A lista de bloqueios de redirecionamento de URL especifica URLs que são redirecionadas para o navegador padrão em execução no endpoint.
8. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
9. Na página Configurações, clique em **Avançar**.
10. Na página Usuários e Máquinas, atribua a política aos Grupos de Entrega aplicáveis e, em seguida, clique em **Avançar**.
11. Na página Resumo, revise as configurações e, em seguida, clique em **Concluir**.

Para habilitar o redirecionamento de URL para todos os aplicativos locais durante a instalação do aplicativo Citrix Workspace, siga estas etapas:

1. Habilite o redirecionamento de URL ao instalar o aplicativo Citrix Workspace para todos os usuários em uma máquina. Isso também registra os complementos do navegador necessários para o redirecionamento de URL.
2. No prompt de comando, execute o comando apropriado para instalar o aplicativo Citrix Workspace usando uma das seguintes opções:
   - Para CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Para CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

### Habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo

> **Nota:**

- Antes de habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, adicione os arquivos de modelo receiver.admx/adml ao GPO local.
- Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Modelos Administrativos > Componentes Citrix > Citrix Workspace** somente quando você adiciona o CitrixBase.admx/CitrixBase.adml à pasta %systemroot%\policyDefinitions.

Para habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá para **Configuração do Computador > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Clique em **Configurações de Acesso a Aplicativos Locais**.
4. Selecione **Habilitado** e, em seguida, selecione **Permitir Redirecionamento de URL**. Para redirecionamento de URL, registre os complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais adiante neste artigo.

### Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o SDK do PowerShell.

Para o Editor do Registro, consulte O Acesso a Aplicativos Locais para aplicativos publicados na lista de recursos gerenciados por meio do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina onde o Delivery Controller™ está sendo executado.
2. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Para ter acesso a **Adicionar Aplicativo de Acesso a Aplicativos Locais** em uma implantação de serviço em nuvem, use o SDK do PowerShell Remoto do Citrix DaaS. Para obter mais informações, consulte SDK do PowerShell Remoto do Citrix DaaS.

1. Baixe o instalador:

`<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. Execute estes comandos:
   a. `asnp citrix.*`.
   b. `Get-XdAuthentication`
3. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Depois de concluir as etapas anteriores aplicáveis, siga estas etapas para continuar.

1. Faça login no Web Studio e selecione **Aplicativos** no painel esquerdo.
2. No painel superior central, clique com o botão direito na área em branco e selecione **Adicionar Aplicativo de Acesso a Aplicativos Locais** no menu de contexto. Você também pode clicar em **Adicionar Aplicativo de Acesso a Aplicativos Locais** na barra de ações. Para exibir a opção Adicionar Aplicativo de Acesso a Aplicativos Locais na barra de ações, clique em **Atualizar**.
3. Publique o aplicativo Local App Access.
   - O assistente de Acesso a Aplicativos Locais é iniciado com uma página de Introdução, que você pode remover de futuras inicializações do assistente.
   - O assistente o guiará pelas páginas Grupos, Localização, Identificação, Entrega e Resumo, descritas abaixo. Ao terminar cada página, clique em **Next** até chegar à página Resumo.
   - Na página Grupos, selecione um ou mais Delivery Groups onde os novos aplicativos serão adicionados e, em seguida, clique em **Next**.
   - Na página Localização, digite o caminho executável completo do aplicativo na máquina local do usuário e digite o caminho para a pasta onde o aplicativo está localizado. A Citrix recomenda que você use o caminho da variável de ambiente do sistema; por exemplo, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
   - Na página Identificação, aceite os valores padrão ou digite as informações desejadas e, em seguida, clique em **Next**.
   - Na página Entrega, configure como este aplicativo é entregue aos usuários e então clique em **Avançar**. Você pode especificar o ícone para o aplicativo selecionado. Você também pode especificar se o atalho para o aplicativo local na área de trabalho virtual está visível no menu Iniciar, na área de trabalho ou em ambos.

- Na página Resumo, revise as configurações e, em seguida, clique em **Finish** para sair do assistente de Acesso a Aplicativos Locais.

### Registrar complementos do navegador

> **Nota:**

> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente quando você instala o aplicativo Citrix Workspace a partir da linha de comando usando a opção /ALLOW_CLIENTHOSTEDAPPSURL=1.

> Você pode usar os seguintes comandos para registrar e cancelar o registro de um ou todos os complementos:

- Para registrar complementos em um dispositivo cliente: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- Para cancelar o registro de complementos em um dispositivo cliente: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- Para registrar complementos em um VDA: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- Para cancelar o registro de complementos em um VDA: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

Onde \<*browser*> é Internet Explorer, Firefox, Chrome ou Todos.

Por exemplo, o seguinte comando registra os complementos do Internet Explorer em um dispositivo executando o aplicativo Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

O seguinte comando registra todos os complementos em um VDA de SO multissessão do Windows.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

### Intercepção de URL entre navegadores

- Por padrão, o Internet Explorer redireciona a URL especificada. Se a URL não estiver na lista de bloqueio, mas o navegador ou site a redirecionar para outra URL, a URL final não será redirecionada. Ela não é redirecionada mesmo que esteja na lista de bloqueio.

Para que o redirecionamento de URL funcione corretamente, habilite o complemento quando solicitado pelo navegador. Se os complementos que estão usando as opções da Internet ou os complementos no prompt estiverem desabilitados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam os URLs.

Quando um complemento é instalado, o Firefox solicita que você permita ou impeça a instalação do complemento em uma nova página de guia. Permita o complemento para que o recurso funcione.

- O complemento do Chrome sempre redireciona a URL final para a qual se navega, e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desativa a extensão, o recurso de redirecionamento de URL não funciona no Chrome. Se o redirecionamento de URL for necessário no modo de navegação anônima, permita que a extensão seja executada nesse modo nas configurações do navegador.

### Configurar o comportamento do aplicativo local ao fazer logoff e desconectar

> **Nota:**

> Se você não seguir estas etapas para configurar as definições, por padrão, os aplicativos locais continuarão a ser executados quando um usuário fizer logoff ou se desconectar da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.

> Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, consulte Comportamento do aplicativo local ao fazer logoff e desconectar na lista de recursos gerenciados por meio do registro.

# Redirecionamento USB genérico e considerações sobre unidades de cliente

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes com alta latência ou sensíveis à segurança.

A tecnologia HDX oferece **redirecionamento USB genérico** para dispositivos especializados que não possuem suporte otimizado ou onde este é inadequado, por exemplo:

- O dispositivo USB possui recursos mais avançados que não fazem parte do suporte otimizado, como um mouse ou webcam com mais botões.
- Os usuários precisam de funções que não fazem parte do suporte otimizado.
- O dispositivo USB é um dispositivo especializado, como equipamento de teste e medição ou um controlador industrial.
- Um aplicativo requer acesso direto ao dispositivo como um dispositivo USB.
- O dispositivo USB tem apenas um driver Windows disponível. Por exemplo, um leitor de cartão inteligente pode não ter um driver disponível para o aplicativo Citrix Workspace™ para Android.
- A versão do aplicativo Citrix Workspace não oferece suporte otimizado para este tipo de dispositivo USB.

Com o redirecionamento USB genérico:

- Os usuários não precisam instalar drivers de dispositivo no dispositivo do usuário.
- Os drivers de cliente USB são instalados na máquina VDA.

**Importante:**

- O redirecionamento USB genérico pode ser usado em conjunto com o suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as configurações de política de dispositivos USB da Citrix para redirecionamento USB genérico e suporte otimizado.
- A configuração de política da Citrix em Regras de otimização de dispositivo USB do cliente é uma configuração específica para redirecionamento USB genérico, para um

> dispositivo USB em particular. Ela não se aplica ao suporte otimizado conforme descrito aqui.

## Considerações de desempenho para dispositivos USB

A latência da rede e a largura de banda podem afetar a experiência do usuário e a operação do dispositivo USB ao usar o redirecionamento USB genérico para alguns tipos de dispositivos USB. Por exemplo, dispositivos sensíveis ao tempo podem não operar corretamente em links de alta latência e baixa largura de banda. Use o suporte otimizado em vez disso, sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para serem utilizáveis, por exemplo, um mouse 3D (usado com aplicativos 3D que também geralmente exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você poderá mitigar o problema ajustando o uso da largura de banda de outros componentes usando as configurações da política de largura de banda. Para obter mais informações, consulte Configurações da política de largura de banda para redirecionamento de dispositivo USB do cliente e Configurações da política de conexão multi-stream.

## Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartão inteligente, leitores de impressão digital e mesas digitalizadoras de assinatura. Outros dispositivos USB, como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser sensíveis.

Dispositivos USB são frequentemente usados para distribuir malware. A configuração do Citrix Workspace app e do Citrix Virtual Apps and Desktops™ pode reduzir, mas não eliminar, o risco desses dispositivos USB. Essa situação se aplica independentemente de ser usado o redirecionamento USB genérico ou o suporte otimizado.

> **Importante:**
>
> Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX usando TLS ou IPsec.

Habilite o suporte apenas para os dispositivos USB de que você precisa. Configure tanto o redirecionamento USB genérico quanto o suporte otimizado para atender a essa necessidade.

Forneça orientação aos usuários para o uso seguro de dispositivos USB:

- Use apenas dispositivos USB obtidos de uma fonte confiável.
- Não deixe dispositivos USB sem supervisão em ambientes abertos — por exemplo, um pen drive em um cybercafé.
- Explique os riscos de usar um dispositivo USB em mais de um computador.

## Compatibilidade com redirecionamento USB genérico

O redirecionamento USB genérico é compatível com dispositivos USB 2.0 e anteriores. O redirecionamento USB genérico também é compatível com dispositivos USB 3.0 conectados a uma porta USB 2.0 ou USB 3.0. O redirecionamento USB genérico não oferece suporte a recursos USB introduzidos no USB 3.0, como super velocidade.

Estes aplicativos Citrix Workspace suportam o redirecionamento USB genérico:

- Citrix Workspace app para Windows, consulte Configurar a entrega de aplicativos.
- Citrix Workspace app para Mac, consulte Citrix Workspace app para Mac.
- Citrix Workspace app para Linux, consulte Otimizar.
- Citrix Workspace app para Chrome OS, consulte Citrix Workspace app para Chrome.

Para versões do Citrix Workspace app, consulte a matriz de recursos do Citrix Workspace app.

Se você estiver usando versões anteriores do Citrix Workspace app, consulte a documentação do Citrix Workspace app para confirmar se o redirecionamento genérico de USB é compatível. Consulte a documentação do Citrix Workspace app para quaisquer restrições sobre os tipos de dispositivos USB compatíveis.

O redirecionamento genérico de USB é compatível com sessões de desktop do VDA para SO de sessão única, da versão 7.6 até a atual.

O redirecionamento genérico de USB é compatível com sessões de desktop do VDA para SO de múltiplas sessões, da versão 7.6 até a atual, com estas restrições:

- O VDA deve estar executando Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o Host de Sessão da Área de Trabalho Remota (RDSH) para o SO do VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não são compatíveis com o redirecionamento genérico de USB porque não seria útil redirecioná-los:

- Modems USB.
- Adaptadores de rede USB.
- Hubs USB. Os dispositivos USB conectados a hubs USB são tratados individualmente.
- Portas COM virtuais USB. Use o redirecionamento de porta COM em vez do redirecionamento genérico de USB.

Para obter informações sobre dispositivos USB que foram testados com o redirecionamento genérico de USB, consulte Citrix Ready Marketplace. Alguns dispositivos USB não funcionam corretamente com o redirecionamento genérico de USB.

## Configurar o redirecionamento USB genérico

Você pode controlar e configurar separadamente quais tipos de dispositivos USB usam o redirecionamento USB genérico:

- No VDA, usando as configurações de política do Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações de política de dispositivos USB na referência de configurações de política
- No aplicativo Citrix Workspace, usando mecanismos dependentes do aplicativo Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações de registro que configuram o aplicativo Citrix Workspace para Windows. Por padrão, o redirecionamento USB é permitido para certas classes de dispositivos USB e negado para outras. Para obter mais informações, consulte Configurar na documentação do aplicativo Citrix Workspace para Windows.

Essa configuração separada oferece flexibilidade. Por exemplo:

- Se duas organizações ou departamentos diferentes forem responsáveis pelo aplicativo Citrix Workspace e pelo VDA, eles poderão impor o controle separadamente. Essa configuração se aplica quando um usuário em uma organização acessa um aplicativo em outra organização.

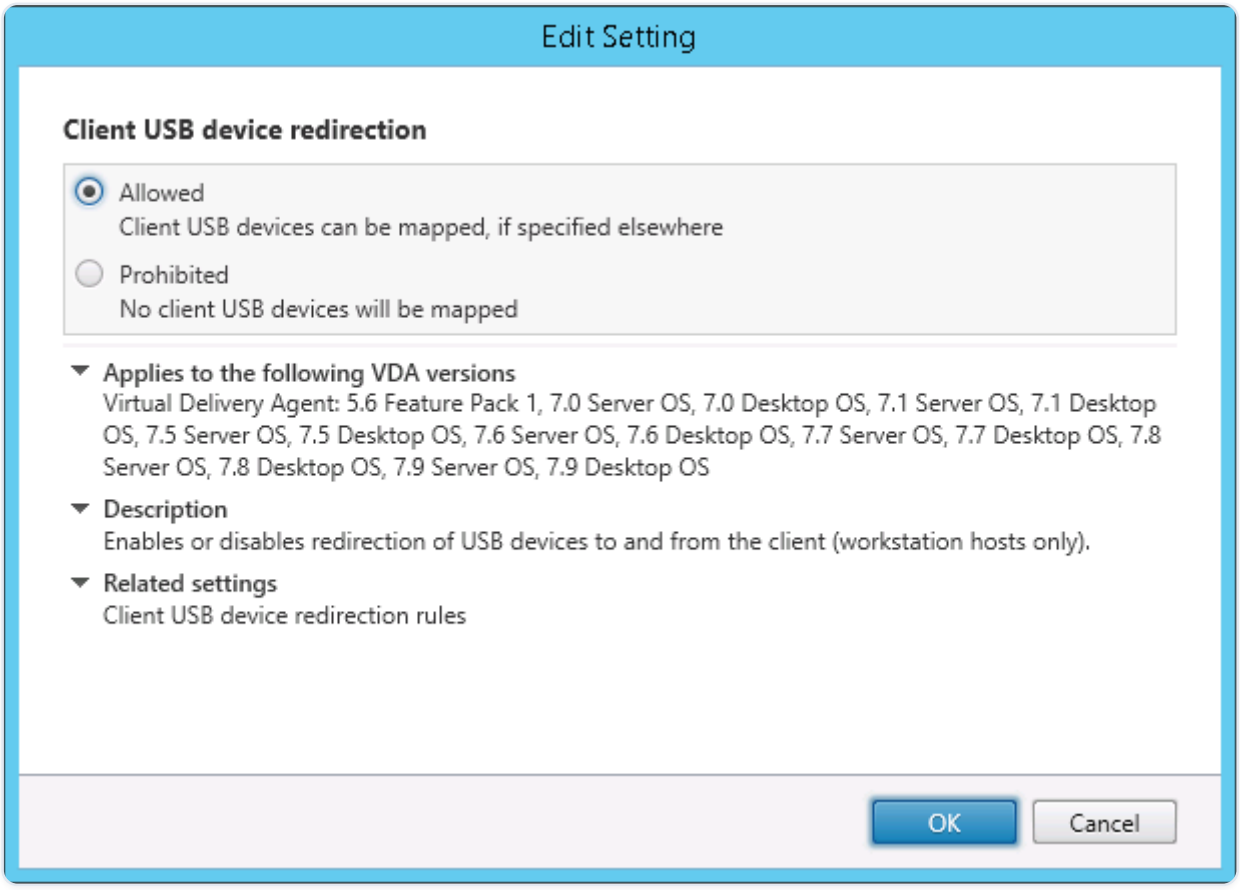
- As configurações de política do Citrix podem controlar dispositivos USB que são permitidos apenas para determinados usuários ou para usuários que se conectam apenas por uma LAN (em vez de usar o Citrix Gateway).

## Habilitar o redirecionamento USB genérico

Para habilitar o redirecionamento USB genérico e não exigir o redirecionamento manual pelo usuário, configure as configurações de política do Citrix e as preferências de conexão do aplicativo Citrix Workspace.

Nas configurações de política do Citrix:

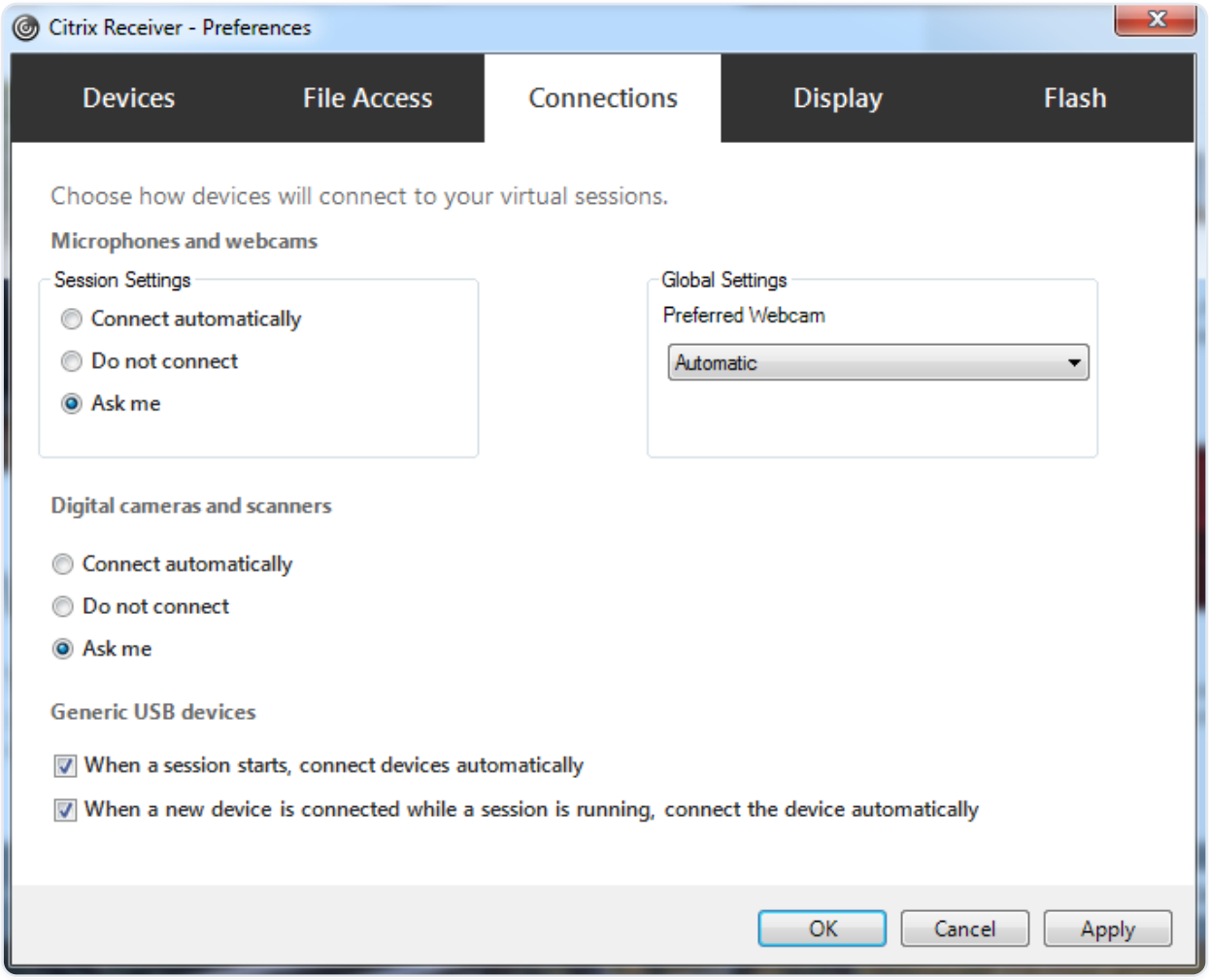
1. Adicione o Redirecionamento de dispositivo USB do cliente a uma política e defina seu valor como **Permitido**.




2. (Opcional) Para atualizar a lista de dispositivos USB disponíveis para redirecionamento, adicione a configuração Regras de redirecionamento de dispositivo USB do cliente a uma política e especifique as regras de política USB.

   Depois que as configurações de política estiverem concluídas, no aplicativo Citrix Workspace:

3. Especifique que os dispositivos sejam conectados automaticamente sem redirecionamento manual. Você pode fazer isso usando um modelo administrativo ou no aplicativo Citrix Workspace para **Windows > Preferências > Conexões**.



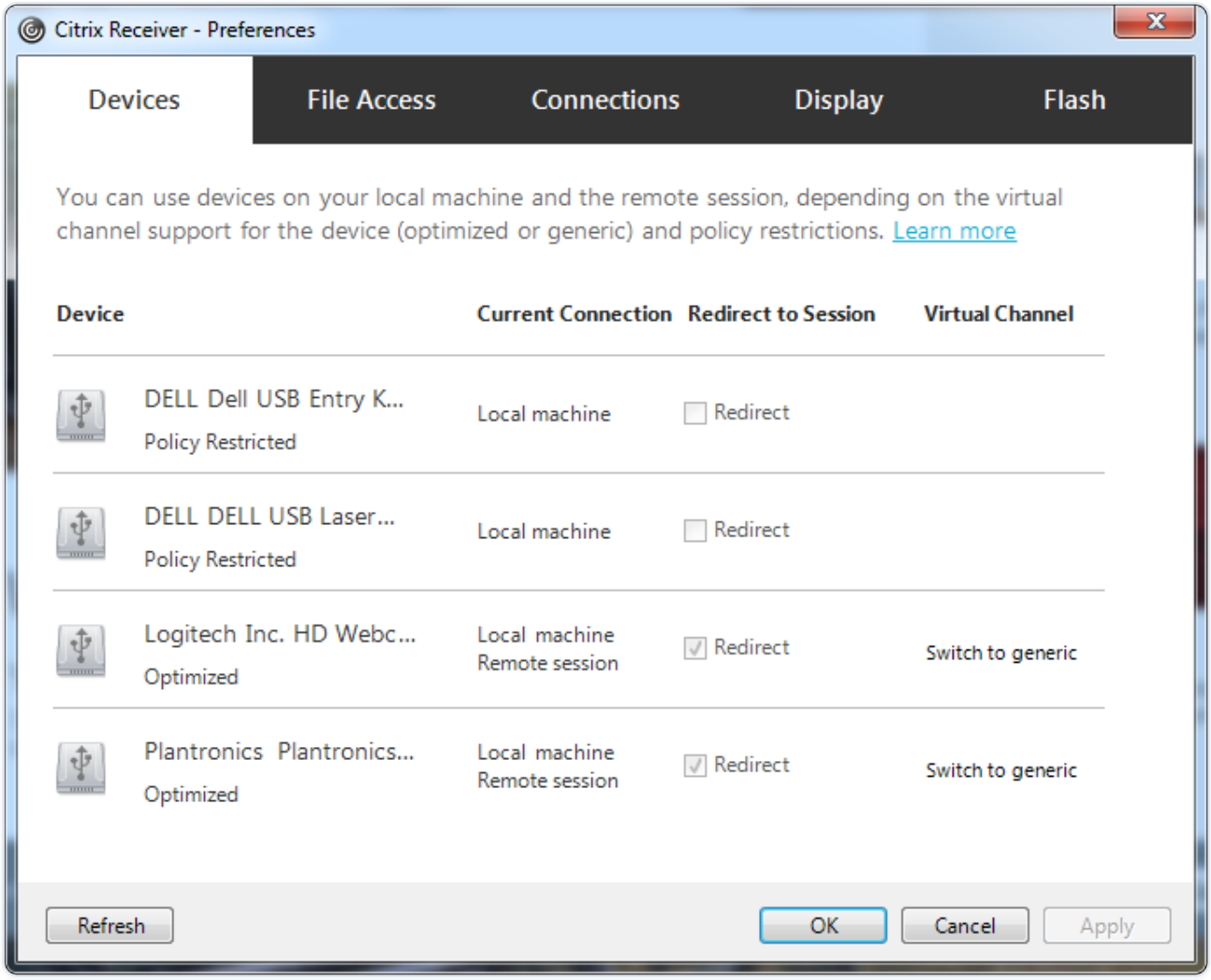

Se você especificou as regras de política USB para o VDA na etapa anterior, especifique as mesmas regras de política para o aplicativo Citrix Workspace.

Para thin clients, consulte o fabricante para obter detalhes sobre o suporte USB e qualquer configuração necessária.

## Configurando os tipos de dispositivos USB disponíveis para redirecionamento USB genérico

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado e as configurações de preferência do usuário USB estão definidas para conectar dispositivos USB automaticamente. Os dispositivos USB também são redirecionados automaticamente quando a barra de conexão não está presente.

Os usuários podem redirecionar explicitamente dispositivos que não são redirecionados automaticamente, selecionando os dispositivos na lista de dispositivos USB. Para obter mais informações, consulte o artigo de ajuda do usuário do aplicativo Citrix Workspace para Windows, Exibir seus dispositivos no Desktop Viewer.




Para usar o redirecionamento USB genérico em vez do suporte otimizado, você pode:

- No aplicativo Citrix Workspace, selecione manualmente o dispositivo USB para usar o redirecionamento USB genérico, escolha **Mudar para genérico** na guia Dispositivos da caixa de diálogo Preferências.
- Selecione automaticamente o dispositivo USB para usar o redirecionamento USB genérico, configurando o redirecionamento automático para o tipo de dispositivo USB (por exemplo, AutoRedirectStorage=1) e defina as configurações de preferência do usuário USB para conectar dispositivos USB automaticamente. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

**Observação:**

> Configure o redirecionamento USB genérico para uso com uma webcam apenas se a webcam for considerada incompatível com o redirecionamento multimídia HDX.

> Para evitar que os dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e o VDA.

Para o redirecionamento USB genérico, você precisa saber pelo menos a classe e a subclasse do dispositivo USB. Nem todos os dispositivos USB usam sua classe e subclasse de dispositivo USB óbvias. Por exemplo:

- Canetas usam a classe de dispositivo de mouse.
- Leitores de cartão inteligente podem usar a classe de dispositivo definida pelo fornecedor ou HID.

Para um controle mais preciso, você precisa saber o ID do Fornecedor, o ID do Produto e o ID da Versão. Você pode obter essas informações do fornecedor do dispositivo.

> **Importante:**

> Dispositivos USB maliciosos podem apresentar características de dispositivo USB que não correspondem ao seu uso pretendido. As regras de dispositivo não se destinam a impedir esse comportamento.

> Você controla os dispositivos USB disponíveis para redirecionamento USB genérico especificando regras de redirecionamento de dispositivo USB, para substituir as regras de política USB padrão.

Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops):

- Na maioria dos casos, baixe o MSI do Citrix Group Policy Management Console (`CitrixGroupPolicyManagement_x64.msi`) e instale-o em seu sistema Active Directory e, em seguida, gerencie as políticas de grupo do AD. (Não instale o MSI em um VDA.)
- Para o Citrix Workspace app para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: raiz do DVD `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops no local:

- Para o VDA, edite as regras de substituição do administrador para as máquinas de SO de várias sessões por meio de regras de política de grupo. O Group Policy Management Console está incluído na mídia de instalação:
  - x64: raiz do DVD `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: raiz do DVD `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Para o Citrix Workspace app para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: raiz do DVD `\os\lang\Support\Configuration\icaclient_usb.adm`

**Aviso:**

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

As regras padrão do produto são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB. Não edite essas regras padrão do produto. Em vez disso, use-as como um guia para criar regras de substituição do administrador, o que é explicado posteriormente neste artigo. As substituições de GPO são avaliadas antes das regras padrão do produto.

As regras de substituição do administrador são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. As regras de política de GPO têm o formato **{Allow: | Deny:}** seguido por um conjunto de expressões *tag=value* separadas por espaço em branco.

As seguintes tags são suportadas:

| TAG | DESCRIÇÃO |
| --- | --- |
| VID | ID do Fornecedor do descritor do dispositivo |

| TAG | DESCRIÇÃO |
|---|---|
| PID | ID do Produto do descritor do dispositivo |
| REL | ID de Lançamento do descritor do dispositivo |
| Classe | Classe do descritor do dispositivo ou de um descritor de interface; consulte o site da USB em `<http://www.usb.org/>` para obter os Códigos de Classe USB disponíveis |
| Subclasse | Subclasse do descritor do dispositivo ou de um descritor de interface |
| Prot | Protocolo do descritor do dispositivo ou de um descritor de interface |

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por `#`. Um delimitador não é necessário, e o comentário é ignorado para fins de correspondência.
- Linhas em branco e linhas de comentário puras são ignoradas.
- Espaços em branco são usados como separadores, mas não podem aparecer no meio de um número ou identificador. Por exemplo, Deny: Class = 08 SubClass=05 é uma regra válida, mas Deny: Class=0 Sub Class=05 não é.
- As tags devem usar o operador de correspondência =. Por exemplo, VID=1230.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.

**Observação:**

- A partir do Citrix Virtual Apps and Desktops versão 2212, alguns dos dispositivos USB são desabilitados de usar o recurso de Redirecionamento USB Genérico. Você deve adicionar esses dispositivos explicitamente usando seus respectivos ID de Fornecedor (VID) e ID de Produto (PID).

- Se você estiver usando o arquivo de modelo ADM, deverá criar regras em uma única linha, como uma lista separada por ponto e vírgula.

Exemplos:

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para identificadores de fornecedor e produto:

  `Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products`

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para uma classe, subclasse e protocolo definidos:

  `Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices`

## Usar e remover dispositivos USB

Os usuários podem conectar um dispositivo USB antes ou depois de iniciar uma sessão virtual.

Ao usar o aplicativo Citrix Workspace para Windows, o seguinte se aplica:

- Dispositivos conectados após o início de uma sessão aparecem imediatamente no menu USB do Desktop Viewer.
- Se um dispositivo USB não estiver sendo redirecionado corretamente, você pode tentar resolver o problema esperando para conectar o dispositivo até depois que a sessão virtual for iniciada.
- Para evitar perda de dados, use o ícone "Remover Hardware com Segurança" do Windows antes de remover o dispositivo USB.

## Controles de segurança para dispositivos de armazenamento em massa USB

É fornecido suporte otimizado para dispositivos de armazenamento em massa USB. Este suporte faz parte do mapeamento de unidades cliente do Citrix Virtual Apps and Desktops. As unidades no dispositivo do usuário são automaticamente mapeadas para letras de unidade na área de trabalho virtual quando os usuários fazem logon. As unidades são exibidas como pastas compartilhadas que possuem letras de unidade mapeadas. Para configurar o mapeamento de unidades cliente,

use a configuração **Unidades removíveis do cliente**. Esta configuração está na seção Configurações de política de redirecionamento de arquivo das configurações de política ICA.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidades cliente ou o redirecionamento USB genérico, ou ambos. Controle-os usando políticas Citrix. As principais diferenças são:

| RECURSO | MAPEAMENTO DE UNIDADE CLIENTE | REDIRECIONAMENTO USB GENÉRICO |
|---|---|---|
| Habilitado por padrão | Sim | Não |
| Acesso somente leitura configurável | Sim | Não |
| Acesso a dispositivo criptografado | Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado | Sim |
| Dispositivos BitLocker To Go | Não | Não |
| Seguro para excluir dispositivo durante uma sessão | Não | Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura |

Se as políticas de redirecionamento USB genérico e de mapeamento de unidades cliente estiverem habilitadas e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidades cliente. Quando as políticas de redirecionamento USB genérico e de mapeamento de unidades cliente estiverem habilitadas e um dispositivo for configurado para redirecionamento automático e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o redirecionamento USB genérico. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX123015.

> **Observação:**
>
> O redirecionamento USB é suportado em conexões de menor largura de banda, por exemplo, 50 Kbps. No entanto, a cópia de arquivos grandes não funciona.

# Imprimir

Gerenciar impressoras em seu ambiente é um processo de várias etapas:

1. Familiarize-se com os conceitos de impressão, se ainda não o fez.
2. Planeje sua arquitetura de impressão. Isso inclui analisar suas necessidades de negócios, sua infraestrutura de impressão existente, como seus usuários e aplicativos interagem com a impressão hoje e qual modelo de gerenciamento de impressão melhor se aplica ao seu ambiente.
3. Configure seu ambiente de impressão selecionando um método de provisionamento de impressora e, em seguida, criando políticas para implantar seu design de impressão. Atualize as políticas quando novos funcionários ou servidores forem adicionados.
4. Teste uma configuração de impressão piloto antes de implantá-la para os usuários.
5. Mantenha seu ambiente de impressão Citrix® gerenciando drivers de impressora e otimizando o desempenho da impressão.
6. Solucione problemas que possam surgir.

## Conceitos de impressão

Antes de começar a planejar sua implantação, certifique-se de entender estes conceitos essenciais para a impressão:

- Os tipos de provisionamento de impressora disponíveis
- Como os trabalhos de impressão são roteados
- Os fundamentos do gerenciamento de drivers de impressora

Os conceitos de impressão baseiam-se nos conceitos de impressão do Windows. Para configurar e gerenciar com sucesso a impressão em seu ambiente, você deve entender como a impressão de rede e cliente do Windows funciona e como isso se traduz em comportamento de impressão neste ambiente.

# Processo de impressão

Neste ambiente, toda a impressão é iniciada (pelo usuário) em máquinas que hospedam aplicativos. Os trabalhos de impressão são redirecionados através do servidor de impressão de rede ou do dispositivo do usuário para o dispositivo de impressão.

Não há um espaço de trabalho persistente para usuários de desktops e aplicativos virtuais. Quando uma sessão termina, o espaço de trabalho do usuário é excluído, portanto, todas as configurações precisam ser reconstruídas no início de cada sessão. Como resultado, cada vez que um usuário inicia uma nova sessão, o sistema deve reconstruir o espaço de trabalho do usuário.

Quando um usuário imprime:

- Determina quais impressoras fornecer ao usuário. Isso é conhecido como provisionamento de impressoras.
- Restaura as preferências de impressão do usuário.
- Determina qual impressora é a padrão para a sessão.

Você pode personalizar como executar essas tarefas configurando opções para provisionamento de impressoras, roteamento de trabalhos de impressão, retenção de propriedades de impressora e gerenciamento de drivers. Certifique-se de avaliar como as várias configurações de opção podem alterar o desempenho da impressão em seu ambiente e a experiência do usuário.

# Provisionamento de impressoras

O processo que torna as impressoras disponíveis em uma sessão é conhecido como provisionamento. O provisionamento de impressoras é tipicamente tratado dinamicamente. Ou seja, as impressoras que aparecem em uma sessão não são predeterminadas e armazenadas. Em vez disso, as impressoras são montadas, com base em políticas, à medida que a sessão é construída durante o logon e a reconexão. Como resultado, as impressoras podem mudar de acordo com a política, localização do usuário e alterações de rede, desde que sejam refletidas nas políticas. Assim, usuários que se deslocam para um local diferente podem ver alterações em seu espaço de trabalho.

O sistema também monitora as impressoras do lado do cliente e ajusta dinamicamente as impressoras criadas automaticamente na sessão com base em adições, exclusões e alterações nas impressoras do lado do cliente. Essa descoberta dinâmica de impressoras beneficia usuários móveis à medida que se conectam de vários dispositivos.

Os métodos mais comuns de provisionamento de impressoras são:

- **Universal Print Server** - O Citrix Universal Print Server fornece suporte de impressão universal para impressoras de rede. O Universal Print Server usa o driver de impressão universal. Essa solução permite que você use um único driver em uma máquina Multi-session OS para permitir a impressão em rede de qualquer dispositivo.

A Citrix recomenda o Citrix Universal™ Print Server para cenários de servidor de impressão remoto. O Universal Print Server transfere o trabalho de impressão pela rede em um formato otimizado e compactado, minimizando assim o uso da rede e melhorando a experiência do usuário.

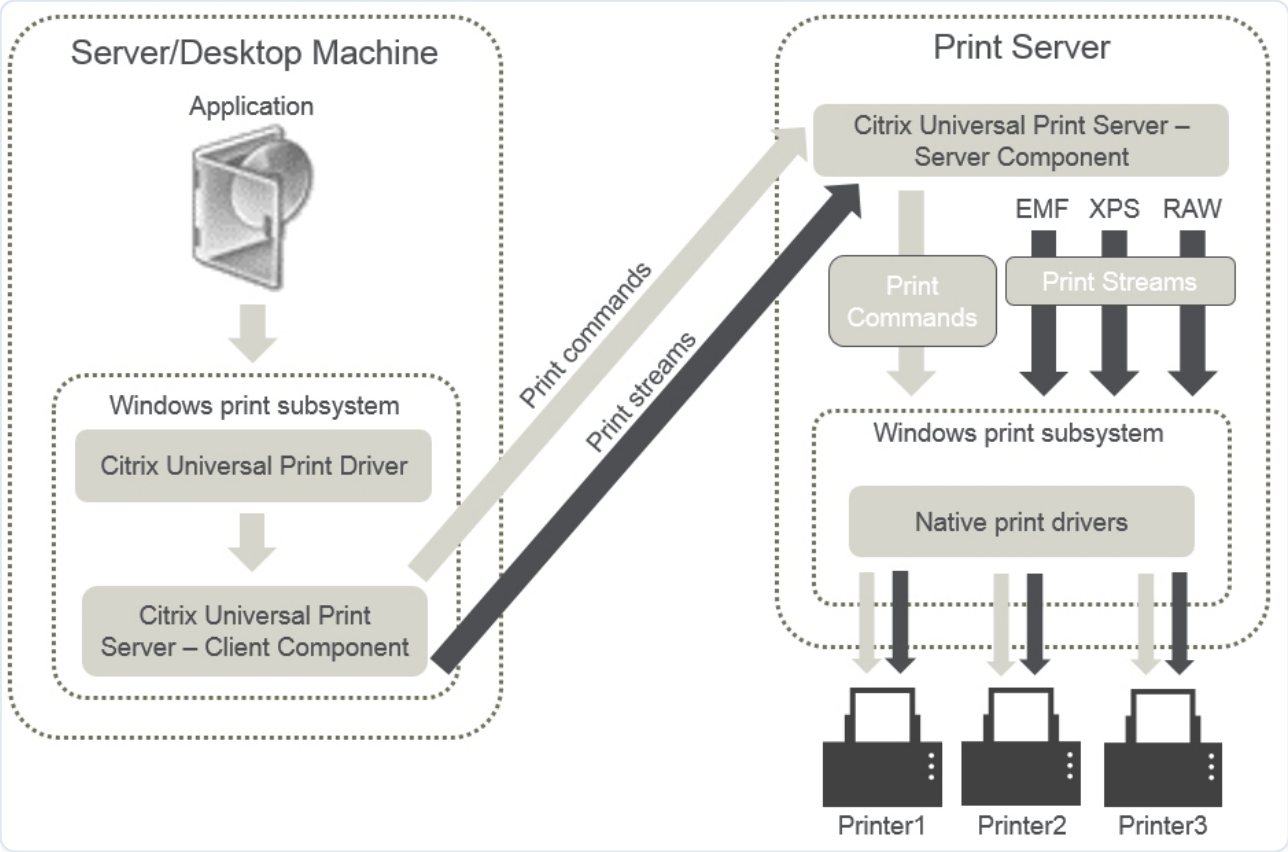
O recurso Universal Print Server compreende:

Um componente cliente, **UPClient** - Habilite o UPClient em cada máquina Multi-session OS que provisiona impressoras de rede de sessão e usa o driver de impressão universal.

Um componente de servidor, **UPServer** - Instale o UPServer em cada servidor de impressão que provisiona impressoras de rede de sessão e usa o driver de impressão Universal para as impressoras de sessão (independentemente de as impressoras de sessão serem provisionadas centralmente ou não).

Para requisitos e detalhes de configuração do Universal Print Server, consulte os artigos de requisitos do sistema e instalação.

A ilustração a seguir mostra o fluxo de trabalho típico para uma impressora baseada em rede em um ambiente que usa o Universal Print Server.




Ao habilitar o Citrix Universal Print Server, todas as impressoras de rede conectadas o utilizam automaticamente por meio da descoberta automática.

- **Criação automática** - A *criação automática* refere-se a impressoras criadas automaticamente no início de cada sessão. Tanto as impressoras de rede remotas quanto as impressoras cliente conectadas localmente podem ser criadas automaticamente. Considere a criação automática apenas da impressora cliente padrão para ambientes com um grande número de impressoras por usuário. A criação automática de um número menor de impressoras usa menos sobrecarga (memória e CPU) em máquinas de SO de múltiplas sessões. Minimizar as impressoras criadas automaticamente também pode reduzir os tempos de logon do usuário.

  As impressoras criadas automaticamente são baseadas em:

  - As impressoras instaladas no dispositivo do usuário.
  - Quaisquer políticas que se apliquem à sessão.

    As configurações da política de criação automática permitem limitar o número ou o tipo de impressoras que são criadas automaticamente. Por padrão, as impressoras estão disponíveis nas sessões ao configurar todas as impressoras no dispositivo do usuário automaticamente, incluindo impressoras conectadas localmente e de rede.

  Depois que o usuário encerra a sessão, as impressoras dessa sessão são excluídas.

A criação automática de impressoras cliente e de rede tem manutenção associada. Por exemplo, adicionar uma impressora exige que você:

- Atualize a configuração da política de impressoras de sessão.
- Adicione o driver a todas as máquinas de SO de múltiplas sessões usando a configuração da política de mapeamento e compatibilidade de driver de impressora.

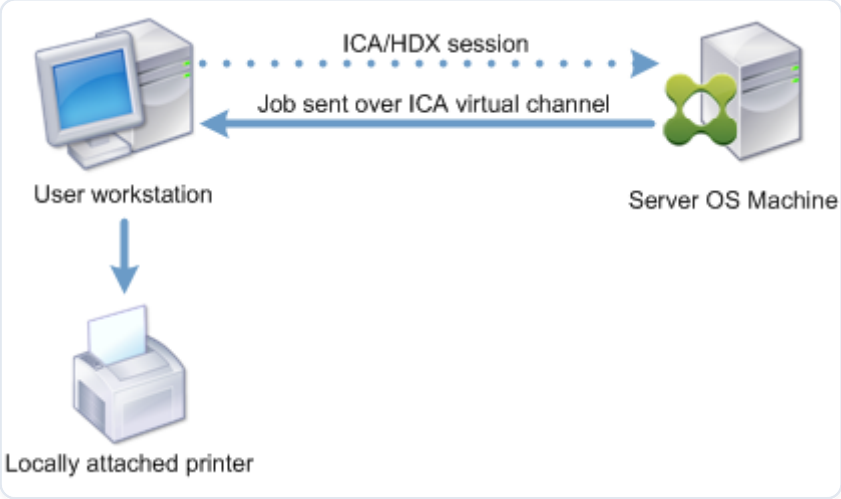
# Roteamento de trabalhos de impressão

O termo caminho de impressão abrange tanto o caminho pelo qual os trabalhos de impressão são roteados quanto o local onde os trabalhos de impressão são armazenados em spool. Ambos os aspectos deste conceito são importantes. O roteamento afeta o tráfego de rede. O spooling afeta a utilização de recursos locais no dispositivo que processa o trabalho.

Nesse ambiente, os trabalhos de impressão podem seguir dois caminhos para um dispositivo de impressão: através do cliente ou através de um servidor de impressão de rede. Esses caminhos são chamados de caminho de impressão do cliente e caminho de impressão de rede. O caminho escolhido por padrão depende do tipo de impressora utilizada.

## Impressoras conectadas localmente

O sistema roteia trabalhos para impressoras conectadas localmente a partir da máquina do SO de múltiplas sessões, através do cliente e, em seguida, para o dispositivo de impressão. O protocolo ICA® otimiza e compacta o tráfego de trabalhos de impressão. Quando um dispositivo de impressão está conectado localmente ao dispositivo do usuário, os trabalhos de impressão são roteados pelo canal virtual ICA.



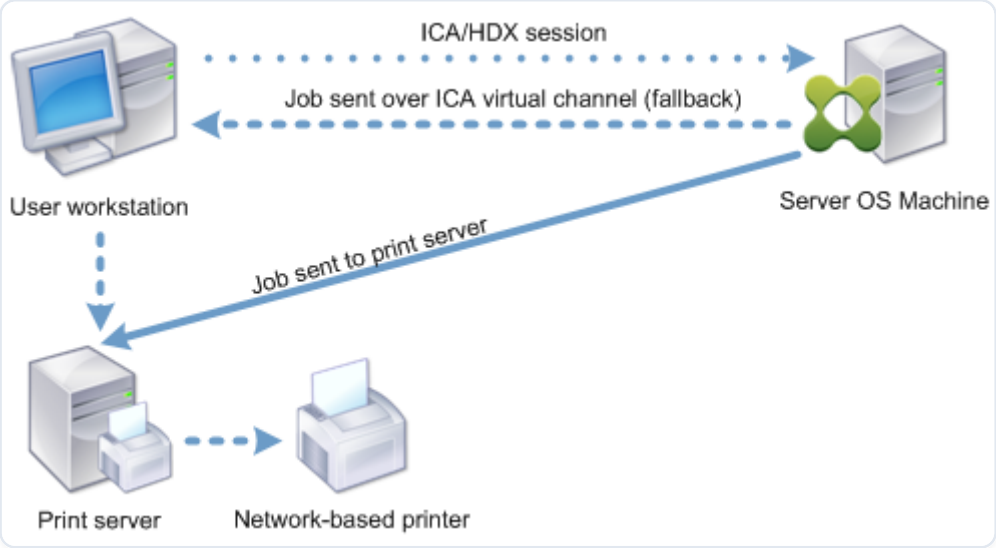
## Impressoras baseadas em rede

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina do SO de múltiplas sessões, através da rede e diretamente para o servidor de impressão. No entanto, os trabalhos de impressão são automaticamente roteados pela conexão ICA nas seguintes situações:

- Se o desktop virtual ou aplicativo não conseguir contatar o servidor de impressão.
- Se o driver de impressora nativo não estiver disponível na máquina do SO de múltiplas sessões.

Se o Universal Print Server não estiver habilitado, configurar o caminho de impressão do cliente para impressão em rede é útil para conexões de baixa largura de banda, como redes de longa distância, que podem se beneficiar da otimização e compressão de tráfego resultantes do envio de trabalhos pela conexão ICA.

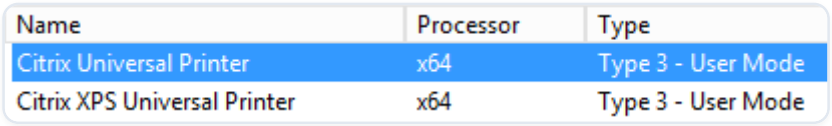
O caminho de impressão do cliente também permite limitar o tráfego ou restringir a largura de banda alocada para trabalhos de impressão. Se o roteamento de trabalhos através do dispositivo do usuário não for possível, como para thin clients sem recursos de impressão, a Qualidade de Serviço deve ser configurada para priorizar o tráfego ICA/HDX e garantir uma boa experiência de usuário na sessão.




# Gerenciamento de driver de impressão

O Citrix Universal Printer Driver (UPD) é um driver de impressão independente de dispositivo, compatível com a maioria das impressoras. O Citrix UPD consiste em dois componentes:

**Componente do servidor**. O Citrix UPD é instalado como parte da instalação do VDA do Citrix Virtual Apps and Desktops™. O VDA instala os seguintes drivers com o Citrix UPD: "Citrix Universal Printer" (driver EMF) e o "Citrix XPS Universal Printer" (driver XPS).



| Name | Processor | Type |
|---|---|---|
| Citrix Universal Printer | x64 | Type 3 - User Mode |
| Citrix XPS Universal Printer | x64 | Type 3 - User Mode |

Os instaladores do VDA não oferecem mais opções para controlar a instalação do driver de impressora PDF do Universal Print Server. O driver de impressora PDF agora é sempre instalado automaticamente. Ao atualizar para o VDA 7.17 (ou uma versão posterior compatível), qualquer driver de impressora PDF Citrix instalado anteriormente é automaticamente removido e substituído pela versão mais recente.

Quando um trabalho de impressão é iniciado, o driver registra a saída do aplicativo e a envia, sem qualquer modificação, para o dispositivo de ponto de extremidade.

**Componente cliente**. O Citrix UPD é instalado como parte da instalação do aplicativo Citrix Workspace™. Ele busca o fluxo de impressão de entrada para a sessão do Citrix Virtual Apps and Desktops. Em seguida, ele encaminha o fluxo de impressão para o subsistema de impressão local, onde o trabalho de impressão é renderizado usando os drivers de impressora específicos do dispositivo.

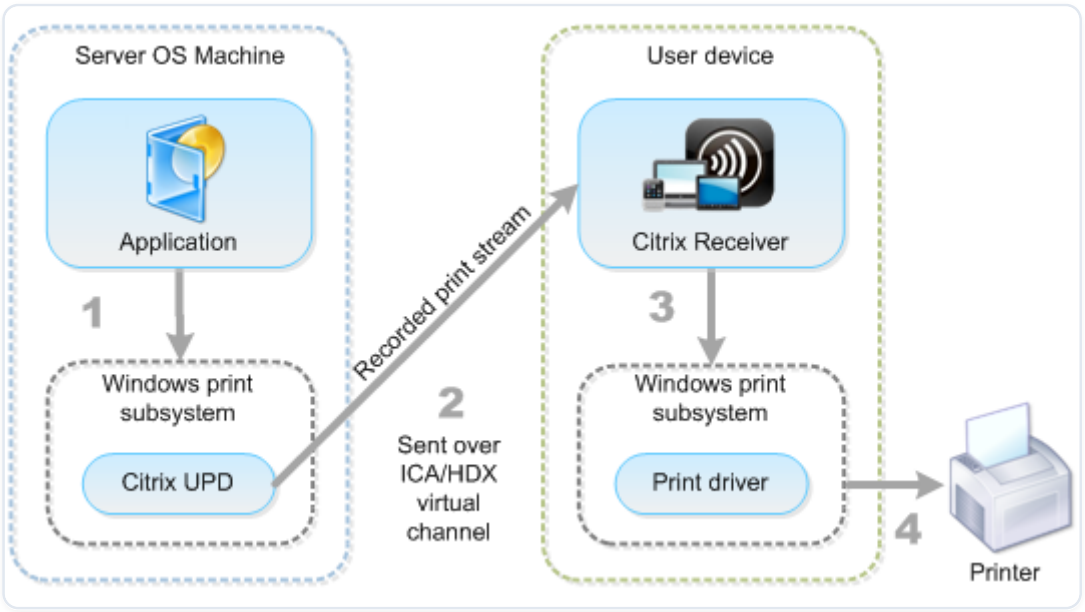
O Citrix UPD oferece suporte aos seguintes formatos de impressão:

- Formato de Metafile Aprimorado (**EMF**), padrão. EMF é a versão de 32 bits do formato Windows Metafile (WMF). O driver EMF só pode ser usado por clientes baseados em Windows.
- Especificação de Papel XML (**XPS**). O driver XPS usa XML para criar um "papel eletrônico" independente de plataforma, semelhante ao formato Adobe PDF.
- Linguagem de Comando de Impressora (**PCL5c** e **PCL4**). PCL é um protocolo de impressão desenvolvido originalmente pela Hewlett-Packard para impressoras a jato de tinta. É usado para imprimir texto e gráficos básicos e é amplamente suportado em periféricos HP LaserJet e multifuncionais.
- PostScript (**PS**). PostScript é uma linguagem de computador que pode ser usada para imprimir texto e gráficos vetoriais. O driver é amplamente utilizado em impressoras de baixo custo e periféricos multifuncionais.

Os drivers PCL e PS são mais adequados ao usar dispositivos não baseados em Windows, como um cliente Mac ou UNIX. A ordem em que o Citrix UPD tenta usar os drivers pode ser alterada usando a configuração de política preferência de driver universal.

O Citrix UPD (drivers EMF e XPS) suporta recursos avançados de impressão, como grampeamento e seleção de origem do papel. Esses recursos estão disponíveis se o driver nativo os disponibilizar usando a tecnologia Microsoft Print Capability. O driver nativo deve usar as Palavras-chave de Esquema de Impressão padronizadas no XML de Capacidades de Impressão. Se forem usadas palavras-chave não padronizadas, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

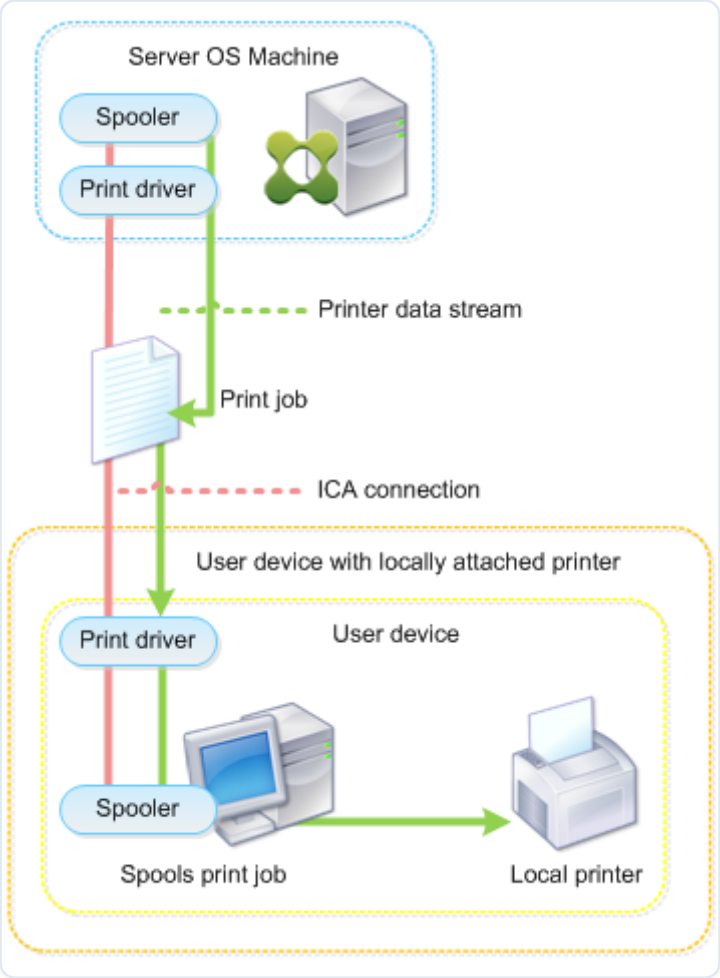
A ilustração a seguir mostra os componentes do driver de impressão universal e um fluxo de trabalho típico para uma impressora conectada localmente a um dispositivo.




Ao planejar sua estratégia de gerenciamento de drivers, determine se você suportará o driver de impressão universal, drivers específicos do dispositivo ou ambos. Se você suportar drivers padrão, deverá determinar:

Durante a autocriação da impressora, se o sistema detectar uma nova impressora local conectada a um dispositivo de usuário, ele verificará a máquina do SO de múltiplas sessões para o driver de impressora necessário. Por padrão, se um driver nativo do Windows não estiver disponível, o sistema usará o driver de impressão universal.

O driver de impressora na máquina Multi-session OS e o driver no dispositivo do usuário devem corresponder para que a impressão seja bem-sucedida. A ilustração a seguir mostra como um driver de impressora é usado em dois locais para impressão de cliente.




- Os tipos de drivers a serem suportados.
- Se deve instalar drivers de impressora automaticamente quando eles estão ausentes das máquinas Multi-session OS.
- Se deve criar listas de compatibilidade de drivers.

## Conteúdo relacionado

- Exemplo de configuração de impressão
- Melhores práticas, considerações de segurança e operações padrão
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

# Exemplo de configuração de impressão

Escolher as opções de configuração de impressão mais apropriadas para suas necessidades e ambiente pode simplificar a administração. Embora a configuração de impressão padrão permita que os usuários imprimam na maioria dos ambientes, os padrões podem não fornecer a experiência de usuário esperada ou o uso de rede ideal e a sobrecarga de gerenciamento para seu ambiente.

Sua configuração de impressão depende de:

- Suas necessidades de negócios e sua infraestrutura de impressão existente.

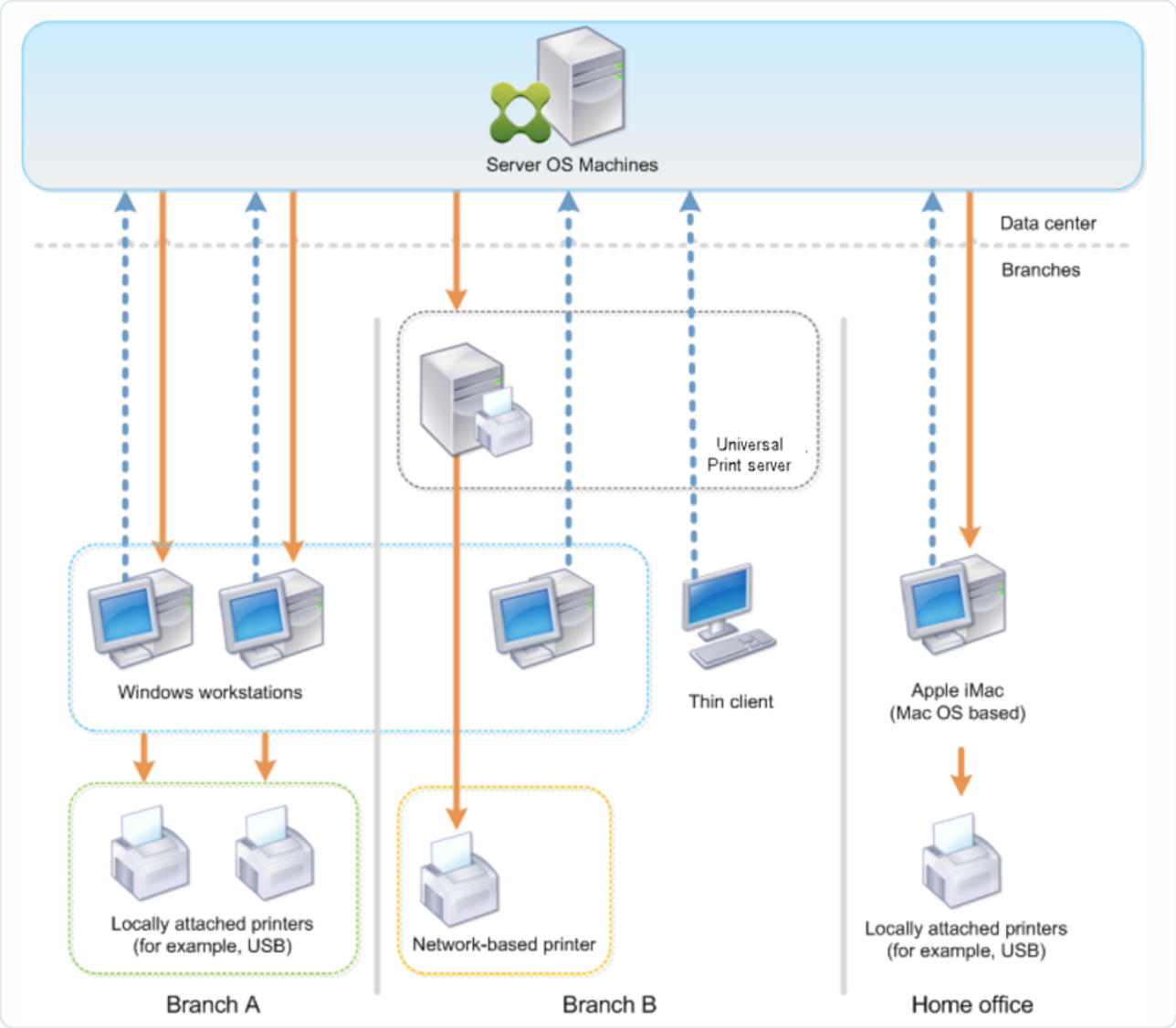
  Projete sua configuração de impressão em torno das necessidades da sua organização. Sua implementação de impressão existente (se os usuários podem adicionar impressoras, quais usuários têm acesso a quais impressoras e assim por diante) pode ser um guia útil ao definir sua configuração de impressão.
- Se sua organização tem políticas de segurança que reservam impressoras para certos usuários (por exemplo, impressoras para Recursos Humanos ou folha de pagamento).
- Se os usuários precisam imprimir enquanto estão longe de seu local de trabalho principal, como trabalhadores que se movem entre estações de trabalho ou viajam a negócios.

Ao projetar sua configuração de impressão, tente dar aos usuários a mesma experiência em uma sessão que eles têm ao imprimir de dispositivos de usuário locais.

## Exemplo de implantação de impressão

A ilustração a seguir mostra a implantação de impressão para estes casos de uso:

- **Filial A** - Um pequeno escritório de filial no exterior com algumas estações de trabalho Windows. Cada estação de trabalho de usuário tem uma impressora privada conectada localmente.
- **Filial B** - Um grande escritório de filial com thin clients e estações de trabalho baseadas em Windows. Para maior eficiência, os usuários desta filial compartilham impressoras baseadas em rede (uma por andar). Servidores de impressão baseados em Windows localizados na filial gerenciam as filas de impressão.
- **Home office** - Um home office com um dispositivo de usuário baseado em Mac OS que acessa a infraestrutura Citrix® da empresa. O dispositivo de usuário tem uma impressora conectada localmente.




As seções a seguir descrevem as configurações que minimizam a complexidade do ambiente e simplificam seu gerenciamento.

## Impressoras cliente criadas automaticamente e driver de impressora Citrix Universal™

Na Filial A, todos os usuários trabalham em estações de trabalho baseadas em Windows, portanto, são usadas impressoras cliente criadas automaticamente e o driver de impressora Universal. Essas tecnologias oferecem os seguintes benefícios:

- Desempenho - Os trabalhos de impressão são entregues pelo canal de impressão ICA®, assim os dados de impressão podem ser compactados para economizar largura de banda.

  Para garantir que um único usuário imprimindo um documento grande não degrade o desempenho da sessão de outros usuários, uma política Citrix é configurada para especificar a largura de banda máxima de impressão.

Uma solução alternativa é aproveitar uma conexão ICA multi-stream, na qual o tráfego de impressão é transferido dentro de uma conexão TCP separada de baixa prioridade. O ICA multi-stream é uma opção quando a Qualidade de Serviço (QoS) não é implementada na conexão WAN.

- Flexibilidade - O uso do driver de impressora Citrix Universal garante que todas as impressoras conectadas a um cliente também possam ser usadas a partir de uma sessão de desktop virtual ou aplicativo sem integrar um novo driver de impressora no data center.

## Servidor de Impressão Universal Citrix

Na Filial B, todas as impressoras são baseadas em rede e suas filas são gerenciadas em um servidor de impressão Windows, portanto, o Servidor de Impressão Universal Citrix é a configuração mais eficiente.

Todos os drivers de impressora necessários são instalados e gerenciados no servidor de impressão por administradores locais. O mapeamento das impressoras para a sessão de desktop virtual ou aplicativo funciona da seguinte forma:

- Para estações de trabalho baseadas em Windows - A equipe de TI local ajuda os usuários a conectar a impressora baseada em rede apropriada às suas estações de trabalho Windows. Isso permite que os usuários imprimam a partir de aplicativos instalados localmente.

  Durante uma sessão de desktop virtual ou aplicativo, as impressoras configuradas localmente são enumeradas por meio de autocriação. O desktop virtual ou aplicativo então se conecta ao servidor de impressão como uma conexão de rede direta, se possível.

  Os componentes do Servidor de Impressão Universal Citrix são instalados e habilitados, portanto, drivers de impressora nativos não são necessários. Se um driver for atualizado ou uma fila de impressora for modificada, nenhuma configuração adicional será necessária no data center.
- Para thin clients - Para usuários de thin client, as impressoras devem ser conectadas dentro da sessão de desktop virtual ou aplicativo. Para fornecer aos usuários a experiência de impressão mais simples, os administradores configuram uma única política de Impressora de Sessão Citrix por andar para conectar a impressora de um andar como a impressora padrão.

  Para garantir que a impressora correta seja conectada mesmo que os usuários se desloquem entre os andares, as políticas são filtradas com base na sub-rede ou no nome do thin client. Essa configuração, referida como impressão por proximidade, permite a manutenção do driver de impressora local (de acordo com o modelo de administração delegada).

Se uma fila de impressora precisar ser modificada ou adicionada, os administradores Citrix devem modificar a respectiva política de impressora de Sessão dentro do ambiente.

Como o tráfego de impressão de rede será enviado fora do canal virtual ICA, o QoS é implementado. O tráfego de rede de entrada e saída nas portas usadas pelo tráfego ICA/HDX é priorizado sobre todo o outro tráfego de rede. Essa configuração garante que as sessões do usuário não sejam impactadas por grandes trabalhos de impressão.

### Impressoras cliente criadas automaticamente e driver de impressora universal Citrix

Para escritórios domésticos onde os usuários trabalham em estações de trabalho não padronizadas e usam dispositivos de impressão não gerenciados, a abordagem mais simples é usar impressoras cliente criadas automaticamente e o driver de impressora universal.

### Resumo da implantação

Em resumo, a implantação de exemplo é configurada da seguinte forma:

- Nenhum driver de impressora é instalado em máquinas com SO de várias sessões. Apenas o driver de impressora universal Citrix é usado. O fallback para impressão nativa e a instalação automática de drivers de impressora estão desabilitados.
- Uma política é configurada para criar automaticamente todas as impressoras cliente para todos os usuários. As máquinas com SO de várias sessões se conectarão diretamente aos servidores de impressão por padrão. A única configuração necessária é habilitar os componentes do Universal Print Server.
- Uma política de impressora de sessão é configurada para cada andar da Filial B e aplicada a todos os thin clients do respectivo andar.
- O QoS é implementado para a Filial B para garantir uma excelente experiência do usuário.

## Melhores práticas, considerações de segurança e operações padrão

### Melhores práticas

Muitos fatores determinam a melhor solução de impressão para um ambiente específico. Algumas dessas melhores práticas podem não se aplicar ao seu Site.

- Use o Citrix Universal™ Print Server.

- Use o driver de impressora Universal ou drivers nativos do Windows.
- Minimize o número de drivers de impressora instalados em máquinas OS de múltiplas sessões.
- Use o mapeamento de drivers para drivers nativos.
- Nunca instale drivers de impressora não testados em um site de produção.
- Evite atualizar um driver. Sempre tente desinstalar um driver, reiniciar o servidor de impressão e, em seguida, instalar o driver de substituição.
- Desinstale drivers não utilizados ou use a política de mapeamento e compatibilidade de drivers de impressora para evitar que impressoras sejam criadas com o driver.
- Tente evitar usar drivers de modo kernel versão 2.
- Para determinar se um modelo de impressora é suportado, entre em contato com o fabricante ou consulte o guia de produtos Citrix Ready em www.citrix.com/ready.

  Em geral, todos os drivers de impressora fornecidos pela Microsoft são testados com os Serviços de Terminal e garantidos para funcionar com o Citrix. No entanto, antes de usar um driver de impressora de terceiros, consulte o fornecedor do driver de impressora para que o driver seja certificado para os Serviços de Terminal pelo programa Windows Hardware Quality Labs (WHQL). A Citrix não certifica drivers de impressora.

## Considerações de segurança

As soluções de impressão Citrix são seguras por design.

- O Serviço Citrix Print Manager monitora e responde constantemente a eventos de sessão, como logon e logoff, desconexão, reconexão e encerramento de sessão. Ele lida com solicitações de serviço, personificando o usuário real da sessão.
- A impressão Citrix atribui a cada impressora um namespace exclusivo em uma sessão.
- A impressão Citrix define o descritor de segurança padrão para impressoras criadas automaticamente para garantir que as impressoras cliente criadas automaticamente em uma sessão sejam inacessíveis a usuários executando em outras sessões. Por padrão, usuários administrativos não podem imprimir acidentalmente em uma impressora cliente de outra sessão, mesmo que possam ver e ajustar manualmente as permissões para qualquer impressora cliente.

## Operações de impressão padrão

Por padrão, se você não configurar nenhuma regra de política, o comportamento de impressão é o seguinte:

- O Universal Print Server está desabilitado.
- Todas as impressoras configuradas no dispositivo do usuário são criadas automaticamente no início de cada sessão.

  Este comportamento é equivalente a configurar a definição de política Citrix Auto-create client printers com a opção Auto-create all client printers.
- O sistema roteia todos os trabalhos de impressão enfileirados para impressoras anexadas localmente a dispositivos de usuário como trabalhos de impressão de cliente (ou seja, sobre o canal ICA® e através do dispositivo do usuário).
- O sistema roteia todos os trabalhos de impressão enfileirados para impressoras de rede diretamente de máquinas Multi-session OS. Se o sistema não conseguir rotear os trabalhos pela rede, ele os roteará através do dispositivo do usuário como um trabalho de impressão de cliente redirecionado.

  Este comportamento é equivalente a desabilitar a definição de política Citrix Direct connection to print servers.
- O sistema tenta armazenar as propriedades de impressão, uma combinação das preferências de impressão do usuário e das configurações específicas do dispositivo de impressão, no dispositivo do usuário. Se o cliente não suportar esta operação, o sistema armazena as propriedades de impressão em perfis de usuário na máquina Multi-session OS.

  Este comportamento é equivalente a configurar a definição de política Citrix Printer properties retention com a opção Held in profile only if not saved on client.
- Em VDAs versão 7.16 e posteriores, a definição de política Citrix "Automatic installation of inbox printer drivers" não tem efeito em versões do Windows 8 e sistemas operacionais Windows posteriores porque os drivers de impressora V3 in-box não estão incluídos no sistema operacional.
- Em VDAs anteriores a 7.16, o sistema usa a versão Windows do driver da impressora se estiver disponível na máquina Multi-session OS. Se o driver da impressora não estiver disponível, o sistema tenta instalar o driver do sistema operacional Windows. Se o driver não estiver disponível no Windows, ele usa um driver de impressão universal Citrix.

Este comportamento é equivalente a habilitar a definição de política Citrix "Automatic installation of in-box printer drivers" e configurar a definição de Universal printing com a opção "Use universal printing only if requested driver is unavailable".

Habilitar "Instalação automática de drivers de impressora internos" pode resultar na instalação de um grande número de drivers de impressora nativos.

**Observação:**

Se você não tiver certeza sobre quais são os padrões de envio para impressão, exiba-os criando uma nova política e definindo todas as regras de política de impressão como Habilitadas. A opção que aparece é o padrão.

### Registro Sempre Ativo

Um recurso de registro Sempre Ativo está disponível para o servidor de impressão e o subsistema de impressão no VDA.

Para agrupar os logs como um ZIP para envio por e-mail, ou para carregar logs automaticamente para o Citrix Insight Services, use o cmdlet PowerShell **Start-TelemetryUpload**.

## Políticas e preferências de impressão

Quando os usuários acessam impressoras de aplicativos publicados, você pode configurar políticas Citrix® para especificar:

- Como as impressoras são provisionadas (ou adicionadas às sessões)
- Como os trabalhos de impressão são roteados
- Como os drivers de impressora são gerenciados

Você pode ter diferentes configurações de impressão para diferentes dispositivos de usuário, usuários ou quaisquer outros objetos nos quais as políticas são filtradas.

A maioria das funções de impressão é configurada através das configurações de política de impressão do Citrix. As configurações de impressão seguem o comportamento padrão da política do Citrix.

O sistema pode gravar as configurações da impressora no objeto da impressora no final de uma sessão ou em um dispositivo de impressão cliente, desde que a conta de rede do usuário tenha

permissões suficientes. Por padrão, o aplicativo Citrix Workspace™ usa as configurações armazenadas no objeto da impressora na sessão, antes de procurar em outros locais por configurações e preferências.

Por padrão, o sistema armazena, ou retém, as propriedades da impressora no dispositivo do usuário (se suportado pelo dispositivo) ou no perfil do usuário na máquina Multi-session OS. Quando um usuário altera as propriedades da impressora durante uma sessão, essas alterações são atualizadas no perfil do usuário na máquina. Na próxima vez que o usuário fizer logon ou se reconectar, o dispositivo do usuário herdará essas configurações retidas. Ou seja, as alterações nas propriedades da impressora no dispositivo do usuário não afetam a sessão atual até que o usuário faça logoff e, em seguida, faça logon novamente.

## Locais de preferência de impressão

Em ambientes de impressão Windows, as alterações feitas nas preferências de impressão podem ser armazenadas no computador local ou em um documento. Neste ambiente, quando os usuários modificam as configurações de impressão, as configurações são armazenadas nestes locais:

- **No próprio dispositivo do usuário** - Os usuários do Windows podem alterar as configurações do dispositivo no dispositivo do usuário clicando com o botão direito do mouse na impressora no Painel de Controle e selecionando Preferências de Impressão. Por exemplo, se Paisagem for selecionado como orientação da página, paisagem será salvo como a preferência de orientação da página padrão para essa impressora.
- **Dentro de um documento** - Em programas de processamento de texto e editoração eletrônica, as configurações do documento, como a orientação da página, são frequentemente armazenadas dentro dos documentos. Por exemplo, quando você enfileira um documento para imprimir, o Microsoft Word geralmente armazena as preferências de impressão que você especificou, como a orientação da página e o nome da impressora, dentro do documento. Essas configurações aparecem por padrão na próxima vez que você imprimir esse documento.
- **De alterações feitas por um usuário durante uma sessão** - O sistema mantém apenas as alterações nas configurações de impressão de uma impressora criada automaticamente se a alteração foi feita no Painel de Controle na sessão; ou seja, na máquina Multi-session OS.
- **Na máquina Multi-session OS** - Estas são as configurações padrão associadas a um driver de impressora específico na máquina.

As configurações preservadas em qualquer ambiente baseado em Windows variam de acordo com onde o usuário fez as alterações. Isso também significa que as configurações de impressão que aparecem em um lugar, como em um programa de planilha, podem ser diferentes das que

aparecem em outros, como documentos. Como resultado, as configurações de impressão aplicadas a uma impressora específica podem mudar ao longo de uma sessão.

### Hierarquia de preferências de impressão do usuário

Como as preferências de impressão podem ser armazenadas em vários locais, o sistema as processa de acordo com uma prioridade específica. Além disso, é importante notar que as configurações do dispositivo são tratadas de forma distinta e geralmente têm precedência sobre as configurações do documento.

Por padrão, o sistema sempre aplica quaisquer configurações de impressão que um usuário modificou durante uma sessão (ou seja, as configurações retidas) antes de considerar quaisquer outras configurações. Quando o usuário imprime, o sistema mescla e aplica as configurações padrão da impressora armazenadas na máquina do sistema operacional multissessão com quaisquer configurações de impressora retidas ou do cliente.

### Salvando preferências de impressão do usuário

A Citrix recomenda que você não altere onde as propriedades da impressora são armazenadas. A configuração padrão, que salva as propriedades da impressora no dispositivo do usuário, é a maneira mais fácil de garantir propriedades de impressão consistentes. Se o sistema não conseguir salvar as propriedades no dispositivo do usuário, ele automaticamente reverterá para o perfil do usuário na máquina do sistema operacional multissessão.

Revise a configuração da política de retenção de propriedades da impressora se estes cenários se aplicarem:

- Se você usa plug-ins legados que não permitem que os usuários armazenem propriedades da impressora em um dispositivo de usuário.
- Se você usa perfis obrigatórios em sua rede Windows e deseja reter as propriedades da impressora do usuário.

## Provisionar impressoras

### Citrix Universal™ Servidor de Impressão

Ao determinar a melhor solução de impressão para o seu ambiente, considere o seguinte:

- O Universal Print Server oferece recursos não disponíveis para o Windows Print Provider: cache de imagem e fonte, compactação avançada, otimização e suporte a QoS.

- O driver de impressão Universal suporta as configurações públicas independentes de dispositivo definidas pela Microsoft. Se os usuários precisarem de acesso a configurações de dispositivo específicas de um fabricante de driver de impressão, o Universal Print Server emparelhado com um driver nativo do Windows pode ser a melhor solução. Com essa configuração, você mantém os benefícios do Universal Print Server enquanto fornece aos usuários acesso a funcionalidades especializadas da impressora. Uma desvantagem a considerar é que os drivers nativos do Windows exigem manutenção.
- O Citrix Universal Print Server oferece suporte de impressão universal para impressoras de rede. O Universal Print Server usa o driver de impressão Universal, um único driver na máquina do sistema operacional multi-sessão que permite a impressão local ou em rede a partir de qualquer dispositivo, incluindo thin clients e tablets.

Para usar o Servidor de Impressão Universal com um driver nativo do Windows, habilite o Servidor de Impressão Universal. Por padrão, se o driver nativo do Windows estiver disponível, ele será usado. Caso contrário, o driver de impressão Universal será usado. Para especificar alterações nesse comportamento, como usar apenas o driver nativo do Windows ou apenas o driver de impressão Universal, atualize a configuração da política de uso do driver de impressão Universal.

### Instalar o Servidor de Impressão Universal

Para usar o Universal Print Server, instale o componente UpsServer em seus servidores de impressão, conforme descrito nos documentos de instalação, e configure-o. Para mais informações, consulte Instalar componentes principais e Instalar usando a linha de comando.

Para ambientes onde você deseja implantar o componente UPClient separadamente, por exemplo, com **XenApp 6.5**:

1. Baixe o pacote autônomo do Citrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) para Windows Single-session OS ou Windows Multi-session OS.
2. Extraia o VDA usando as instruções da linha de comando descritas em Instalar usando a linha de comando.
3. Instale os pré-requisitos de `\Image-Full\Support\VcRedist_2013_RTM`
    - Vcredist_x64 / vcredist_x86
        - Execute x86 apenas para 32 bits, e ambos para implantações de 64 bits
4. Instale o pré-requisito cdf de `\Image-Full\x64\Virtual Desktop Components` ou `\Image-Full\x86\Virtual Desktop Components`.
    - Cdf_x64 / Cdf_x86

    - x86 para 32 bits, x64 para 64 bits

5. Encontre o componente UPClient em `\Image-Full\x64\Virtual Desktop Components` ou `\Image-Full\x86\Virtual Desktop Components`.
6. Instale o componente UPClient extraindo e, em seguida, iniciando o MSI do componente.
7. É necessário reiniciar após a instalação do componente UPClient.

### Desativar o CEIP para o Universal Print Server

Você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix ao instalar o Universal Print Server. O primeiro upload de dados ocorre sete dias após a data e hora da instalação.

Para desativar o CEIP, edite a chave de registro **`HKLM\Software\Citrix\Universal Print Server\CEIPEnabled`** e defina o valor **DWORD** como **0**.

Para reativar, defina o valor DWORD como 1.

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

Para obter mais informações, consulte Citrix Insight Services.

### Configurar o Universal Print Server

Use as seguintes configurações de política da Citrix para configurar o Universal Print Server. Para obter mais informações, consulte a ajuda das configurações de política na tela.

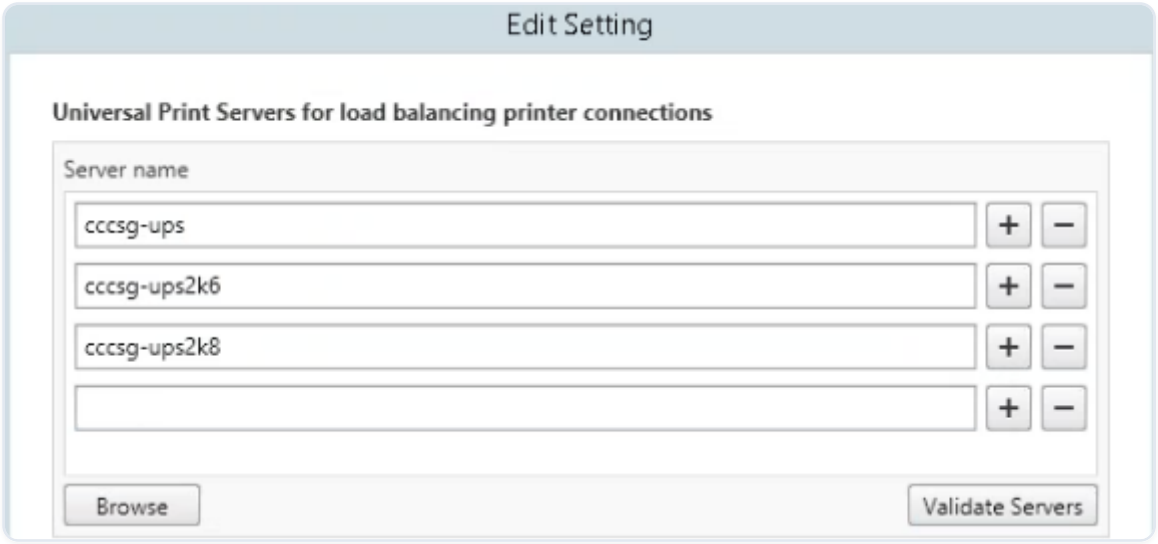
- **Ativar Universal Print Server**. O Universal Print Server é desativado por padrão. Ao ativar o Universal Print Server, você escolhe se deseja usar o Provedor de Impressão do Windows caso o Universal Print Server esteja indisponível. Depois de ativar o Universal Print Server, um usuário pode adicionar e enumerar impressoras de rede por meio das interfaces do Provedor de Impressão do Windows e do Provedor Citrix.
- **Porta do fluxo de dados de impressão do Universal Print Server (CGP)**. Especifica o número da porta TCP usado pelo ouvinte CGP (Common Gateway Protocol) do fluxo de dados de impressão do Universal Print Server. O padrão é **7229**.
- **Porta do serviço web do Universal Print Server (HTTP/SOAP)**. Especifica o número da porta TCP usado pelo ouvinte do Universal Print Server para solicitações HTTP/SOAP de entrada. O padrão é **8080**.

Para alterar a porta padrão HTTP 8080 para a comunicação do Universal Print Server com os VDAs do Citrix Virtual Apps and Desktops, o seguinte registro também deve ser criado e o valor do número da porta modificado nos computadores do Universal Print Server:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

Este número de porta deve corresponder à Política HDX, porta do serviço web do Universal Print Server (HTTP/SOAP), no Studio.

- **Limite de largura de banda de entrada do fluxo de impressão do Universal Print Server (kbps)**. Especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão entregues de cada trabalho de impressão para o Universal Print Server usando CGP. O padrão é 0 (ilimitado).
- **Universal Print Servers para balanceamento de carga**. Esta configuração lista os Universal Print Servers a serem usados para balancear a carga das conexões de impressora estabelecidas no início da sessão, após avaliar outras configurações de política de impressão do Citrix. Para otimizar o tempo de criação da impressora, a Citrix recomenda que todos os servidores de impressão tenham o mesmo conjunto de impressoras compartilhadas.




- **Limite de Universal Print Servers fora de serviço**. Especifica quanto tempo o balanceador de carga deve esperar por um servidor de impressão indisponível para se recuperar antes de determinar que o servidor está permanentemente offline e redistribuir sua carga para outros servidores de impressão disponíveis. O padrão é 180 (segundos).

Uma vez que as políticas de impressão são modificadas no Delivery Controller™, pode levar alguns minutos para que as alterações de política sejam aplicadas aos VDAs.

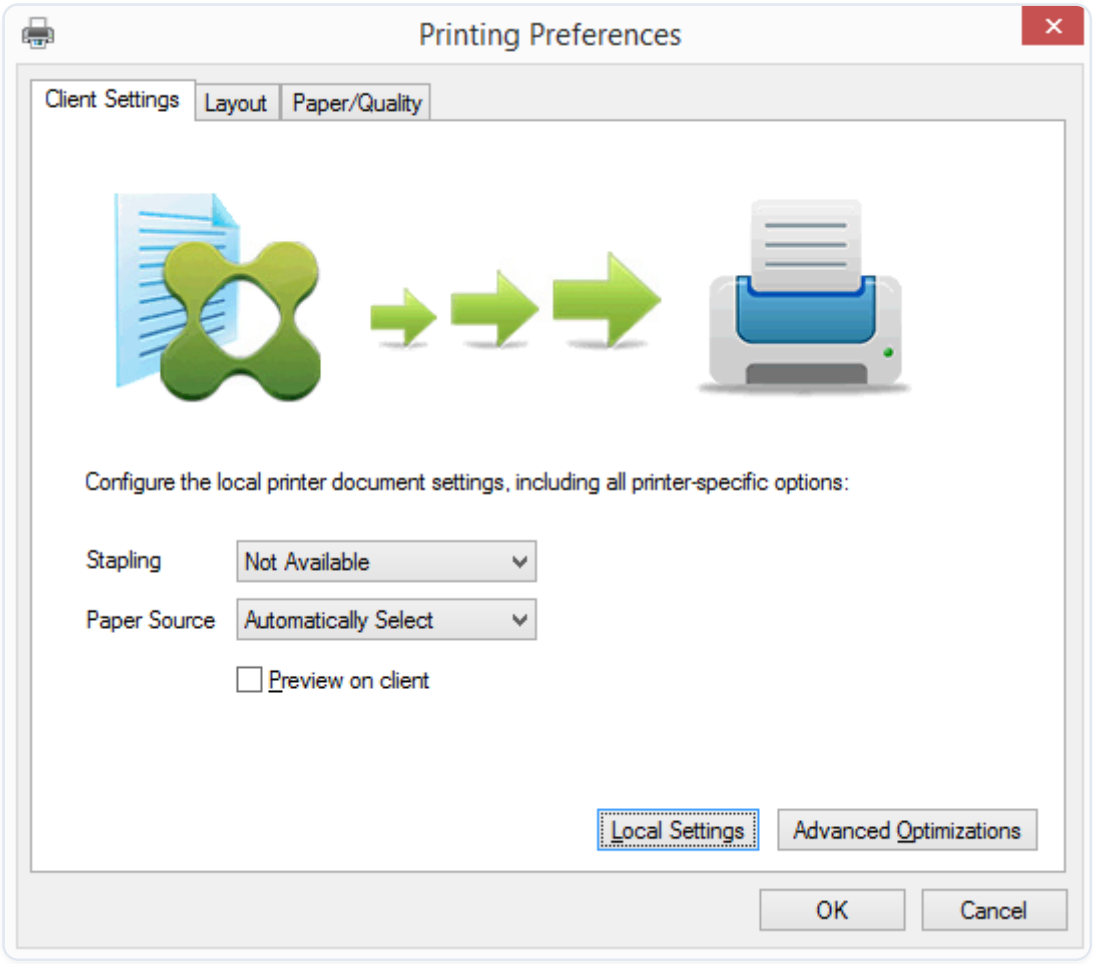
**Interações com outras configurações de política** - O Universal Print Server respeita outras configurações de política de impressão do Citrix e interage com elas conforme observado na tabela a seguir. As informações fornecidas pressupõem que a configuração de política do Universal Print Server esteja habilitada, os componentes do Universal Print Server estejam instalados e as configurações de política sejam aplicadas.

| Configuração de política | Interação |
|---|---|
| Redirecionamento de impressora cliente, Criação automática de impressoras cliente | Depois que o Universal Print Server é habilitado, as impressoras de rede cliente são criadas usando o driver de impressão Universal em vez dos drivers nativos. Os usuários veem o mesmo nome de impressora de antes. |
| Impressoras de sessão | Ao usar a solução Citrix Universal Print Server, as configurações de política do driver de impressão universal são respeitadas. |
| Conexões diretas com o servidor de impressão | Quando o Universal Print Server está ativado e a configuração de política de uso do driver de impressão universal está configurada para usar apenas a impressão universal, uma conexão direta de impressora de rede pode ser criada com o servidor de impressão, usando o driver de impressão universal. |
| Preferência de UPD | Suporta drivers EMF e XPS. |

**Efeitos nas interfaces do usuário** - O driver de impressão universal Citrix usado pelo Universal Print Server desativa os seguintes controles de interface do usuário:

- Na caixa de diálogo Propriedades da Impressora, o botão Configurações Locais da Impressora
- Na caixa de diálogo Propriedades do Documento, os botões Configurações Locais da Impressora e Visualizar no cliente

O driver de impressão universal Citrix (drivers EMF e XPS) suporta recursos avançados de impressão, como grampeamento e origem do papel. O usuário pode selecionar as opções de Grampeamento ou Origem do Papel na caixa de diálogo de impressão UPD personalizada se as impressoras cliente ou de rede mapeadas para o UPD na sessão suportarem esses recursos.




Para definir configurações de impressora não padrão, como grampeamento e PIN seguro, selecione **Configurações Locais** na caixa de diálogo de impressão UPD do cliente para quaisquer impressoras cliente mapeadas que usem drivers Citrix UPD EMF ou XPS. A caixa de diálogo **Preferências de Impressão** da impressora mapeada é exibida fora da sessão no cliente, permitindo que o usuário altere qualquer opção da impressora, e as configurações de impressora modificadas são usadas na sessão ativa ao imprimir esse documento.

Esses recursos estão disponíveis se o driver nativo os disponibilizar usando a tecnologia Microsoft Print Capability. O driver nativo deve usar as palavras-chave padronizadas do Print Schema no XML de Print Capabilities. Se forem usadas palavras-chave não padrão, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

Ao usar o Universal Print Server, o Assistente para Adicionar Impressora do Citrix Print Provider é o mesmo que o Assistente para Adicionar Impressora do Windows Print Provider, com as seguintes exceções:

- Ao adicionar uma impressora por nome ou endereço, você pode fornecer um número de porta HTTP/SOAP para o servidor de impressão. Esse número de porta se torna parte do nome da impressora e aparece nas exibições.

- Se a configuração da política de uso do driver de impressão universal Citrix especificar que a impressão universal deve ser usada, o nome do driver de impressão universal aparecerá ao selecionar uma impressora. O Provedor de Impressão do Windows não pode usar o driver de impressão universal.

O Provedor de Impressão Citrix não oferece suporte à renderização do lado do cliente.

Para obter mais informações sobre o Universal Print Server, consulte CTX200328.

## Impressoras cliente criadas automaticamente

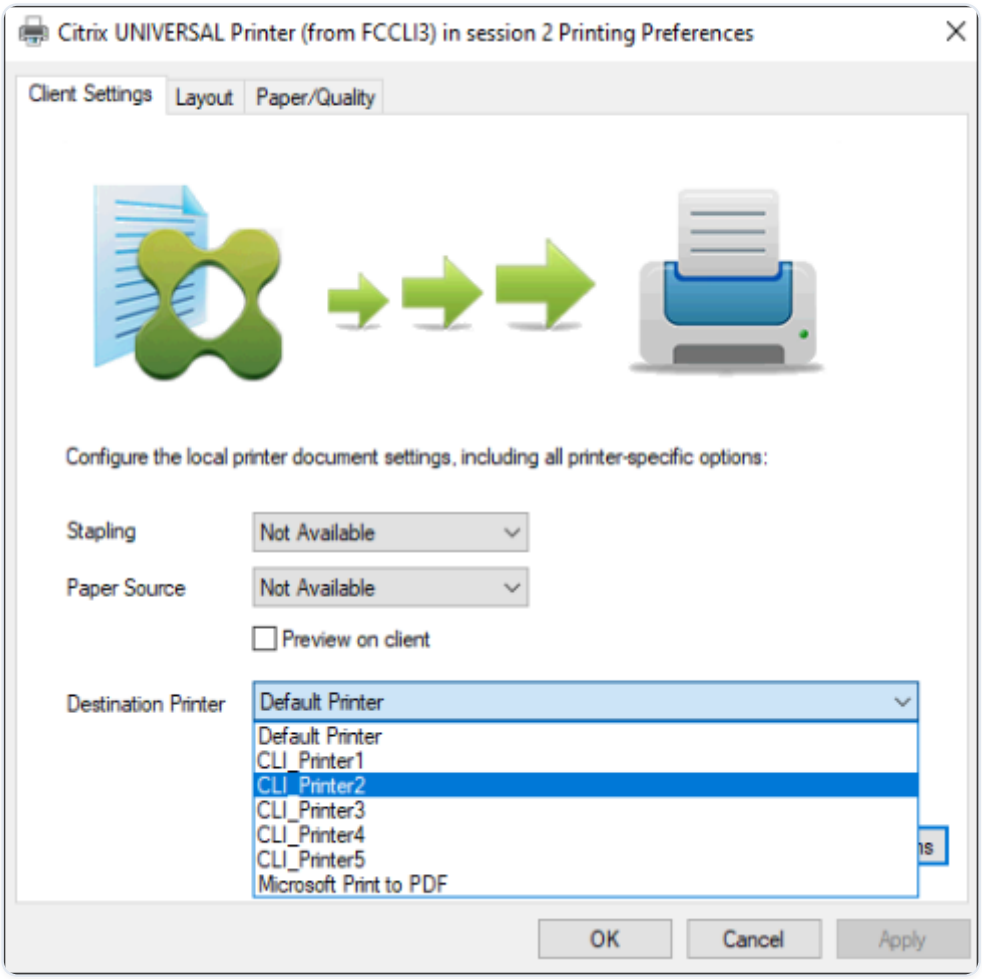
Estas soluções de impressão universal são fornecidas para impressoras cliente:

- **Citrix Universal Printer** - Uma impressora genérica criada no início das sessões que não está vinculada a um dispositivo de impressão. Ao criar automaticamente e usar apenas a Citrix Universal Printer, você pode experimentar menor uso de recursos e tempos de logon do usuário. A Universal Printer pode imprimir em qualquer dispositivo de impressão do lado do cliente.

  A Citrix Universal Printer pode não funcionar para todos os dispositivos de usuário ou aplicativos Citrix Workspace™ em seu ambiente. A Citrix Universal Printer requer um ambiente Windows e não oferece suporte ao Citrix Offline Plug-in ou a aplicativos transmitidos para o cliente. Considere usar impressoras cliente criadas automaticamente e o driver de impressão universal para esses ambientes.

  Para usar uma solução de impressão universal para aplicativos Citrix Workspace que não sejam Windows, use um dos outros drivers de impressão universais baseados em Postscript ou PCL.

  A Citrix Universal Printer permite selecionar a impressora padrão do cliente ou uma impressora cliente específica como destino de impressão. Para escolher uma impressora específica para um trabalho de impressão, abra a caixa de diálogo **Preferências de Impressão**. Selecione o menu suspenso **Impressora de Destino**. A opção **Impressora Padrão** envia trabalhos de impressão para a impressora padrão do cliente. Quaisquer impressoras redirecionadas do cliente anexadas ao endpoint que executa a sessão também são listadas. A impressora que você selecionar é salva como a impressora de destino para quaisquer trabalhos de impressão futuros.




- **Drivers de impressão universais Citrix** - Um driver de impressora independente de dispositivo. Se você configurar um driver de impressão universal Citrix, o sistema usará o driver de impressão universal baseado em EMF por padrão.

  O driver de impressão universal Citrix pode criar trabalhos de impressão menores do que drivers de impressora mais antigos ou menos avançados. No entanto, um driver específico do dispositivo pode ser necessário para otimizar trabalhos de impressão para uma impressora especializada.

**Configurar impressão universal** - Use as seguintes configurações de política Citrix para configurar a impressão universal. Para obter mais informações, consulte a ajuda das configurações de política na tela.

- Uso do driver de impressão universal. Especifica quando usar a impressão universal.
- Criar automaticamente impressora universal genérica. Habilita ou desabilita a criação automática do objeto de impressora universal genérica Citrix para sessões quando um dispositivo de usuário compatível com Impressão Universal está em uso. Por padrão, o objeto de impressora universal genérica não é criado automaticamente.

- Preferência de driver universal. Especifica a ordem em que o sistema tenta usar drivers de impressão universais, começando com a primeira entrada na lista. Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.
- Preferência de visualização de impressão universal. Especifica se deve usar a função de visualização de impressão para impressoras universais genéricas ou criadas automaticamente.
- Modo de processamento EMF de impressão universal. Controla o método de processamento do arquivo de spool EMF no dispositivo de usuário Windows. Por padrão, os registros EMF são enviados diretamente para a impressora. O envio direto para a impressora permite que o spooler processe os registros mais rapidamente e use menos recursos da CPU.

Para mais políticas, consulte Otimizar o desempenho da impressão. Para alterar os padrões de configurações como tamanho do papel, qualidade de impressão, cor, duplex e o número de cópias, consulte CTX113148.

**Criar impressoras automaticamente a partir do dispositivo do usuário** - No início de uma sessão, o sistema cria automaticamente todas as impressoras no dispositivo do usuário por padrão. Você pode controlar quais tipos de impressoras, se houver, são provisionados para os usuários e impedir a criação automática.

Use a configuração de política do Citrix Criar impressoras cliente automaticamente para controlar a criação automática. Você pode especificar que:

- Todas as impressoras visíveis para o dispositivo do usuário, incluindo impressoras de rede e conectadas localmente, são criadas automaticamente no início de cada sessão (padrão)
- Todas as impressoras locais fisicamente conectadas ao dispositivo do usuário são criadas automaticamente
- Apenas a impressora padrão para o dispositivo do usuário é criada automaticamente
- A criação automática está desabilitada para todas as impressoras cliente

A configuração Criar impressoras cliente automaticamente exige que a configuração Redirecionamento de impressora cliente esteja Permitida (o padrão).

## Atribuir impressoras de rede aos usuários

Por padrão, as impressoras de rede no dispositivo do usuário são criadas automaticamente no início das sessões. O sistema permite reduzir o número de impressoras de rede que são

enumeradas e mapeadas, especificando as impressoras de rede a serem criadas em cada sessão. Essas impressoras são chamadas de impressoras de sessão.

Você pode filtrar políticas de impressora de sessão por endereço IP para fornecer impressão por proximidade. A impressão por proximidade permite que os usuários dentro de um intervalo de endereço IP especificado acessem automaticamente os dispositivos de impressão de rede que existem dentro do mesmo intervalo. A impressão por proximidade é fornecida pelo Citrix Universal Print Server e não requer a configuração descrita nesta seção.

A impressão por proximidade pode envolver o seguinte cenário:

- A rede interna da empresa opera com um servidor DHCP que designa automaticamente endereços IP aos usuários.
- Todos os departamentos da empresa possuem faixas de endereços IP designadas exclusivas.
- As impressoras de rede existem dentro da faixa de endereços IP de cada departamento.

Quando a impressão por proximidade é configurada e um funcionário viaja de um departamento para outro, nenhuma configuração adicional do dispositivo de impressão é necessária. Uma vez que o dispositivo do usuário é reconhecido dentro da nova faixa de endereços IP do departamento, ele terá acesso a todas as impressoras de rede dentro dessa faixa.

**Configurar impressoras específicas para serem redirecionadas em sessões** - Para criar impressoras atribuídas pelo administrador, configure a configuração de política do Citrix Session printers. Adicione uma impressora de rede a essa política usando um dos seguintes métodos:

- Insira o caminho UNC da impressora usando o formato `\\servername\printername`.
- Navegue até um local de impressora na rede.
- Procure impressoras em um servidor específico. Insira o nome do servidor usando o formato `\\servername` e clique em Procurar.

Importante: O servidor mescla todas as configurações de impressora de sessão habilitadas para todas as políticas aplicadas, começando das prioridades mais altas para as mais baixas. Quando uma impressora é configurada em vários objetos de política, as configurações padrão personalizadas são obtidas apenas do objeto de política de maior prioridade no qual essa impressora está configurada.

As impressoras de rede criadas com a configuração Session printers podem variar de acordo com o local onde a sessão foi iniciada, filtrando por objetos como sub-redes.

**Especificar uma impressora de rede padrão para uma sessão** - Por padrão, a impressora principal do usuário é usada como a impressora padrão para a sessão. Use a configuração de política do Citrix Default printer para alterar como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

1. Na página de configurações de Default printer, selecione uma configuração para Escolher a impressora padrão do cliente:
    - Nome da impressora de rede. As impressoras adicionadas com a configuração de política Session printers aparecem neste menu. Selecione a impressora de rede a ser usada como padrão para esta política.
    - Não ajustar a impressora padrão do usuário. Usa a configuração atual do perfil de usuário do Terminal Services ou Windows para a impressora padrão. Para mais informações, consulte a ajuda das configurações de política na tela.
2. Aplique a política ao grupo de usuários (ou outros objetos filtrados) que você deseja afetar.

**Configurar impressão por proximidade** - A impressão por proximidade também é fornecida pelo Citrix Universal Print Server, que não requer a configuração descrita aqui.

1. Crie uma política separada para cada sub-rede (ou para corresponder ao local da impressora).
2. Em cada política, adicione as impressoras na localização geográfica dessa sub-rede à configuração Impressoras de sessão.
3. Defina a configuração Impressora padrão como Não ajustar a impressora padrão do usuário.
4. Filtre as políticas por endereço IP do cliente. Certifique-se de atualizar essas políticas para refletir as alterações nos intervalos de endereços IP DHCP.

# Manter o ambiente de impressão

A manutenção do ambiente de impressão inclui:

- Gerenciar drivers de impressora
- Otimizar o desempenho da impressão
- Exibir impressora e gerenciar filas de impressão

## Gerenciar drivers de impressora

Para minimizar a sobrecarga administrativa e o potencial de problemas com drivers de impressão, a Citrix recomenda o uso do driver de impressão Citrix Universal™.

Se a criação automática falhar, por padrão, o sistema instala um driver de impressora nativo do Windows fornecido com o Windows. Se um driver não estiver disponível, o sistema retorna ao driver de impressão Universal. Para obter mais informações sobre os padrões do driver de impressora, consulte Melhores práticas, considerações de segurança e operações padrão.

Se o driver de impressão Citrix Universal não for uma opção para todos os cenários, mapeie os drivers de impressora para minimizar a quantidade de drivers instalados em máquinas com SO de múltiplas sessões. Além disso, o mapeamento de drivers de impressora permite que você:

- Permitir que impressoras especificadas usem apenas o driver de impressão Citrix Universal
- Permitir ou impedir que impressoras sejam criadas com um driver especificado
- Substituir drivers de impressora bons por drivers desatualizados ou corrompidos
- Substituir um driver disponível no servidor Windows por um nome de driver de cliente

**Impedir a instalação automática de drivers de impressora** - A instalação automática de drivers de impressão deve ser desabilitada para garantir a consistência entre as máquinas com SO de múltiplas sessões. Isso pode ser alcançado por meio de políticas Citrix®, políticas Microsoft ou ambas. Para impedir a instalação automática de drivers de impressora nativos do Windows, desabilite a configuração de política Citrix Instalação automática de drivers de impressora internos.

**Mapear drivers de impressora cliente** - Cada cliente fornece informações sobre impressoras do lado do cliente durante o logon, incluindo o nome do driver da impressora. Durante a criação automática da impressora cliente, os nomes dos drivers de impressora do servidor Windows são selecionados para corresponder aos nomes dos modelos de impressora fornecidos pelo cliente. O processo de criação automática então usa os drivers de impressora identificados e disponíveis para construir filas de impressão cliente redirecionadas.

Aqui está o processo geral para definir regras de substituição de driver e editar configurações de impressão para drivers de impressora cliente mapeados:

1. Para especificar regras de substituição de driver para impressoras cliente criadas automaticamente, configure a configuração de política do Citrix Mapeamento e compatibilidade de driver de impressora adicionando o nome do driver da impressora cliente e selecionando o driver do servidor que você deseja substituir pelo driver da impressora cliente no menu Localizar driver de impressora. Você pode usar curingas nesta configuração. Por exemplo, para forçar todas as impressoras HP a usar um driver específico, especifique HP* na configuração da política.

2. Para banir um driver de impressora, selecione o nome do driver e escolha a configuração Não criar.
3. Conforme necessário, edite um mapeamento existente, remova um mapeamento ou altere a ordem das entradas de driver na lista.
4. Para editar as configurações de impressão para drivers de impressora cliente mapeados, selecione o driver da impressora, clique em Configurações e especifique configurações como qualidade de impressão, orientação e cor. Se você especificar uma opção de impressão que o driver da impressora não suporta, essa opção não terá efeito. Essa configuração substitui as configurações de impressora retidas que o usuário definiu durante uma sessão anterior.
5. A Citrix recomenda testar o comportamento das impressoras em detalhes após mapear os drivers, já que algumas funcionalidades da impressora podem estar disponíveis apenas com um driver específico.

Quando os usuários fazem logon, o sistema verifica a lista de compatibilidade do driver da impressora cliente antes de configurar as impressoras cliente.

## Otimizar o desempenho da impressão

Para otimizar o desempenho da impressão, use o Servidor de Impressão Universal e o driver de impressão Universal. As seguintes políticas controlam a otimização e a compactação da impressão:

- Padrões de otimização de impressão universal. Especifica as configurações padrão para a Impressora Universal quando ela é criada para uma sessão:
    - Qualidade de imagem desejada especifica o limite padrão de compactação de imagem aplicado à impressão universal. Por padrão, a Qualidade Padrão está ativada, o que significa que os usuários só podem imprimir imagens usando compactação de qualidade padrão ou reduzida.
    - Ativar compactação pesada ativa ou desativa a redução da largura de banda além do nível de compactação definido pela Qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compactação pesada está desativada.
    - Configurações de cache de imagem e fonte especificam se devem ou não armazenar em cache imagens e fontes que aparecem várias vezes no fluxo de impressão, garantindo que cada imagem ou fonte exclusiva seja enviada à impressora apenas uma vez. Por padrão, imagens e fontes incorporadas são armazenadas em cache.
    - Permitir que não administradores modifiquem essas configurações especifica se os usuários podem ou não alterar as configurações padrão de otimização de impressão

dentro de uma sessão. Por padrão, os usuários não têm permissão para alterar as configurações padrão de otimização de impressão.

- Limite de compactação de imagem de impressão universal. Define a qualidade máxima e o nível mínimo de compactação disponíveis para imagens impressas com o driver de impressão Universal. Por padrão, o limite de compactação de imagem é definido como Melhor Qualidade (compactação sem perdas).
- Limite de qualidade de impressão universal. Especifica o número máximo de pontos por polegada (dpi) disponível para gerar saída impressa na sessão. Por padrão, nenhum limite é especificado.

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina do SO de múltiplas sessões, através da rede e diretamente para o servidor de impressão. Considere rotear trabalhos de impressão pela conexão ICA® se a rede tiver latência substancial ou largura de banda limitada. Para fazer isso, desative a configuração da política Citrix Conexões diretas a servidores de impressão. Os dados enviados pela conexão ICA são compactados, de modo que menos largura de banda é consumida à medida que os dados viajam pela WAN.

**Melhore o desempenho da sessão limitando a largura de banda de impressão** - Ao imprimir arquivos de máquinas do SO de múltiplas sessões para impressoras de usuário, outros canais virtuais (como vídeo) podem ter desempenho reduzido devido à competição por largura de banda, especialmente se os usuários acessarem servidores por meio de redes mais lentas. Para evitar essa degradação, você pode limitar a largura de banda usada pela impressão do usuário. Ao limitar a taxa de transmissão de dados para impressão, você disponibiliza mais largura de banda no fluxo de dados HDX™ para transmissão de vídeo, toques de tecla e dados do mouse.

**Importante:**

O limite de largura de banda da impressora é sempre imposto, mesmo quando nenhum outro canal está em uso.

Use as seguintes configurações de impressora de largura de banda da política Citrix para configurar os limites de largura de banda de impressão da sessão. Para definir os limites para o site, execute esta tarefa usando o Studio. Para definir os limites para servidores individuais, execute esta tarefa usando o Console de Gerenciamento de Política de Grupo no Windows localmente em cada máquina do SO de múltiplas sessões.

- A configuração Limite de largura de banda de redirecionamento de impressora especifica a largura de banda disponível para impressão em kilobits por segundo (kbps).
- A configuração Limite de largura de banda de redirecionamento de impressora em porcentagem limita a largura de banda disponível para impressão a uma porcentagem da largura de banda geral disponível.

  Observação: Para especificar a largura de banda como uma porcentagem usando a configuração Limite de largura de banda de redirecionamento de impressora em porcentagem, habilite também o Limite geral de largura de banda da sessão.

  Se você inserir valores para ambas as configurações, a configuração mais restritiva (o valor mais baixo) será aplicada.

Para obter informações em tempo real sobre a largura de banda de impressão, use o Citrix Director.

## Balancear carga de Universal Print Servers

A solução Universal Print Server pode ser dimensionada adicionando mais servidores de impressão à solução de balanceamento de carga. Não há um único ponto de falha, pois cada VDA tem seu próprio balanceador de carga para distribuir a carga de impressão para todos os servidores de impressão.

Use as configurações de política, Universal Print Servers para balanceamento de carga e Limite de Universal Print Servers fora de serviço, para distribuir a carga de impressão entre todos os servidores de impressão na solução de balanceamento de carga.

Se houver uma falha imprevista de um servidor de impressão, o mecanismo de failover do balanceador de carga em cada VDA redistribui automaticamente as conexões de impressora alocadas nos servidores de impressão com falha para os outros servidores de impressão disponíveis, de modo que todas as sessões existentes e futuras funcionem normalmente sem afetar a experiência do usuário e sem exigir intervenção imediata do administrador.

Os administradores podem monitorar a atividade dos servidores de impressão com balanceamento de carga usando um conjunto de contadores de desempenho para rastrear o seguinte no VDA:

- Lista de servidores de impressão com balanceamento de carga no VDA e seu estado (disponível, indisponível)
- Número de conexões de impressora aceitas por cada servidor de impressão

- Número de conexões de impressora que falharam em cada servidor de impressão
- Número de conexões de impressora ativas em cada servidor de impressão
- Número de conexões de impressora pendentes em cada servidor de impressão

## Exibir e gerenciar filas de impressão

A tabela a seguir resume onde você pode exibir impressoras e gerenciar filas de impressão em seu ambiente.

| | CAMINHO DE IMPRESSÃO | LOCALIZAÇÃO |
|---|---|---|
| Impressoras cliente (Impressoras conectadas ao dispositivo do usuário) | Caminho de impressão do cliente | UAC Ativado: Snap-in de Gerenciamento de Impressão localizado no Microsoft Management Console; UAC Desativado: Pré-Windows 8: Painel de Controle, Windows 8: Snap-in de Gerenciamento de Impressão |
| Impressoras de rede (Impressoras em um servidor de impressão de rede) | Caminho de impressão de rede | UAC Ativado: Servidor de Impressão \> Snap-in de Gerenciamento de Impressão localizado no Microsoft Management Console; UAC Desativado: Servidor de Impressão \> Painel de Controle |
| Impressoras de rede (Impressoras em um servidor de impressão de rede) | Caminho de impressão do cliente | UAC Ativado: Servidor de Impressão \> snap-in de Gerenciamento de Impressão localizado no Console de Gerenciamento da Microsoft; UAC Desativado: Pré-Windows 8: Painel de Controle, Windows 8: snap-in de Gerenciamento de Impressão |
| Impressoras de servidor de rede local (Impressoras de | Caminho de impressão de rede | UAC Ativado: Servidor de Impressão \> Painel de |

| | CAMINHO DE IMPRESSÃO | LOCALIZAÇÃO |
|---|---|---|
| um servidor de impressão de rede que são adicionadas a uma máquina de SO multi-sessão) | | Controle; UAC Desativado: Servidor de Impressão \> Painel de Controle |

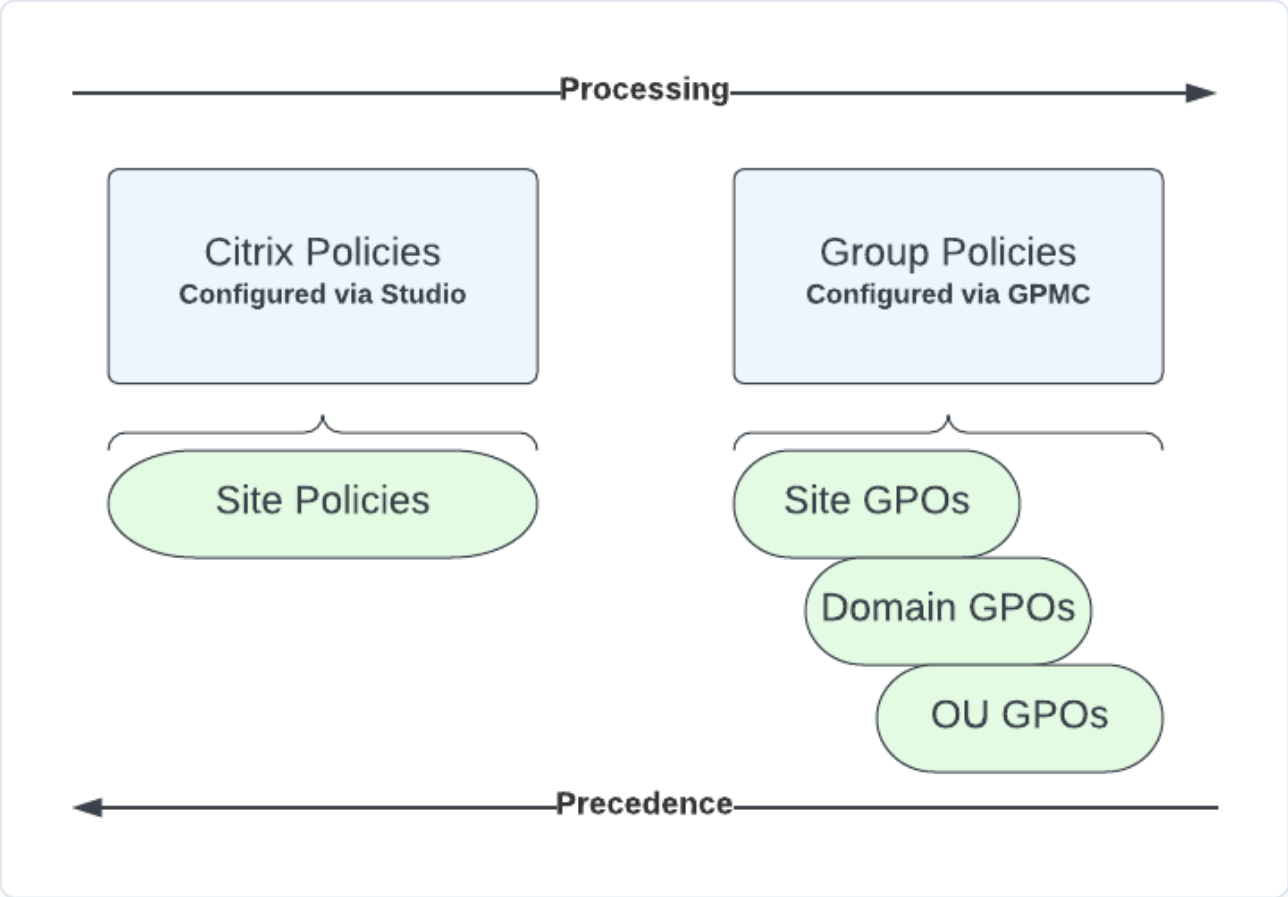
**Nota:**

Filas de impressão para impressoras de rede que usam o caminho de impressão de rede são privadas e não podem ser gerenciadas pelo sistema.

# Políticas

Políticas são uma coleção de configurações que definem como sessões, largura de banda e segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.

Você pode aplicar configurações de política a máquinas físicas e virtuais ou a usuários. Você pode aplicar configurações a usuários individuais no nível local ou em grupos de segurança em um Active Directory. As configurações definem critérios e regras específicas. Se você não atribuir as políticas especificamente, as configurações serão aplicadas a todas as conexões.




Você pode aplicar políticas em diferentes níveis da rede. As configurações de política colocadas no nível de GPO da Unidade Organizacional têm a precedência mais alta na rede. As políticas no nível de GPO de Domínio substituem as políticas no nível de Objeto de Política de Grupo do Site. O nível de Objeto de Política de Grupo do Site substitui quaisquer políticas conflitantes nos níveis de Políticas Locais da Microsoft e da Citrix.

Todas as Políticas Locais da Citrix são criadas e gerenciadas no console do Web Studio e armazenadas no Banco de Dados do Site. As Políticas de Grupo são criadas e gerenciadas usando o Console de Gerenciamento de Política de Grupo da Microsoft (GPMC) e armazenadas no Active Directory. As Políticas Locais da Microsoft são criadas no Sistema Operacional Windows e são armazenadas no registro.

O Studio usa um Assistente de Modelagem para ajudar os administradores a comparar as configurações dentro de modelos e políticas para ajudar a eliminar configurações conflitantes e redundantes. Os administradores podem definir GPOs usando o GPMC para configurar as configurações. Além disso, aplicá-las a um conjunto de usuários-alvo em diferentes níveis da rede.

Esses GPOs são salvos no Active Directory. O acesso ao gerenciamento dessas configurações é restrito para a maioria do pessoal de TI por questões de segurança.

As configurações são mescladas de acordo com a prioridade e sua condição. Qualquer configuração desabilitada substitui uma configuração habilitada de classificação inferior. As configurações de política não configuradas são ignoradas e não substituem as configurações de classificação inferior.

As políticas locais também podem ter conflitos com as políticas de grupo no Active Directory, que podem se sobrepor dependendo da situação.

Todas as políticas são processadas na seguinte ordem:

1. O usuário final faz logon em uma máquina usando credenciais de domínio.
2. As credenciais são enviadas para o controlador de domínio.
3. O Active Directory aplica todas as políticas (usuário final, endpoint, unidade organizacional e domínio).
4. O usuário final faz logon no aplicativo Citrix Workspace™ e acessa um aplicativo ou desktop.
5. As políticas da Citrix e da Microsoft são processadas para o usuário final e a máquina que hospeda o recurso.
6. O Active Directory determina a precedência para as configurações de política. Em seguida, ele as aplica aos registros do dispositivo endpoint e à máquina que hospeda o recurso.
7. O usuário final faz logoff do recurso. As políticas Citrix para o usuário final e o dispositivo de endpoint não estão mais ativas.
8. O usuário final faz logoff do dispositivo do usuário, o que libera as políticas de usuário da GPO.
9. O usuário final desliga o dispositivo, o que libera as políticas de máquina da GPO.

Ao criar políticas para grupos de usuários, dispositivos e máquinas, alguns membros podem ter requisitos diferentes e precisariam de exceções a algumas configurações de política. As exceções são feitas por meio de filtros no Studio e no GPMC que determinam quem ou o que a política afeta.

**Nota:**

Não oferecemos suporte à mistura de políticas do Windows e Citrix na mesma GPO.

# Trabalhar com políticas

**Observação:**

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

Configure as políticas do Citrix para controlar o acesso do usuário e os ambientes de sessão. As políticas do Citrix são o método mais eficiente de controlar as configurações de conexão, segurança e largura de banda. Você pode criar políticas para grupos específicos de usuários, dispositivos ou tipos de conexão. Cada política pode conter várias configurações.

## Ferramentas para trabalhar com políticas do Citrix

Você pode usar as seguintes ferramentas com as políticas do Citrix.

- **Web Studio.** Se você é um administrador Citrix sem permissão para gerenciar a política de grupo, use o Web Studio para criar políticas para seu site. As políticas criadas usando o Web Studio são armazenadas no banco de dados do site, e as atualizações são enviadas para o VDA quando esse VDA se registra com o broker ou quando um usuário se conecta a esse VDA.
- **Editor de Política de Grupo Local** (snap-in do Microsoft Management Console). Se o seu ambiente de rede usa o Active Directory e você tem permissão para gerenciar a política de grupo, você pode usar o Editor de Política de Grupo Local para criar políticas para seu site. As

configurações que você configura afetam os Objetos de Política de Grupo (GPOs) que você especifica no Console de Gerenciamento de Política de Grupo.

**Importante:**

Recomendamos usar o Editor de Política de Grupo Local para configurar algumas configurações de política. Exemplos incluem configurações relacionadas ao registro de VDAs com um controlador e configurações relacionadas a servidores Microsoft App-V. Validações de política adicionais são adicionadas. Como resultado, fazer um upgrade no local pode levar à perda de dados de política se configurações de política inválidas estiverem presentes. Se você criar ou editar as políticas usando um método diferente do Web Studio, a Citrix recomenda que você use a versão mais recente do SDK e do snap-in.

## Ordem de processamento e precedência da política

As configurações da política de grupo são processadas na seguinte ordem:

1. GPO Local
2. GPO do site do Virtual Apps and Desktops (armazenado no banco de dados do Site)
3. GPOs de nível de site
4. GPOs de nível de domínio
5. Unidades Organizacionais

No entanto, se ocorrer um conflito, as configurações de política processadas por último sobrescrevem as configurações processadas anteriormente. A ordem de precedência para as configurações de política é a seguinte:

1. Unidades Organizacionais
2. GPOs de nível de domínio
3. GPOs no nível do site
4. GPO do site do Virtual Apps and Desktops (armazenado no banco de dados do Site)
5. GPO local

Por exemplo, um administrador Citrix usa o Web Studio para criar uma política (Política A) que habilita o redirecionamento de arquivos do cliente para os funcionários de vendas da empresa. Enquanto isso, outro administrador usa o Editor de Política de Grupo para criar uma política (Política B) que desabilita o redirecionamento de arquivos do cliente para os funcionários de

vendas. Quando os funcionários de vendas fazem logon nos desktops virtuais, a Política B é aplicada e a Política A é ignorada. O motivo é que a Política B foi processada no nível do domínio e a Política A foi processada no nível da GPO do site do Virtual Apps and Desktops.

No entanto, quando um usuário inicia uma sessão ICA® ou RDP (Remote Desktop Protocol), as configurações de sessão do Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou usando a Configuração do Host da Sessão da Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão do cliente RDP. Os exemplos de configurações de conexão do cliente RDP são Papel de parede da área de trabalho, animação de menu e Visualizar conteúdo da janela ao arrastar.

Ao usar várias políticas, você pode priorizar políticas que contêm configurações conflitantes. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

## Fluxo de trabalho para políticas Citrix

O processo para configurar políticas é o seguinte:

1. Crie a política.
2. Configure as configurações da política.
3. Atribua a política a objetos de máquina e usuário.
4. Priorize a política.
5. Verifique a política efetiva executando o assistente de Modelagem de Política de Grupo do Citrix.

> **Observação:**
>
> Você abre o assistente de Modelagem de Política de Grupo do Citrix navegando até a guia **Políticas > Modelagem** e clicando em **Iniciar Assistente de Modelagem** na barra de ações. A guia **Modelagem** está disponível no Web Studio mediante solicitação do cliente.

## navegar políticas e configurações do Citrix

No Editor de Política de Grupo Local, as políticas e configurações aparecem em duas categorias: Configuração do Computador e Configuração do Usuário. Cada categoria tem um nó de Políticas

Citrix. Consulte a documentação da Microsoft para obter detalhes sobre como navegar e usar este snap-in.

No Web Studio, as configurações de política são classificadas em categorias com base na funcionalidade ou recurso que afetam. Por exemplo, a seção **Gerenciamento de Perfil** inclui configurações de política para Gerenciamento de Perfil.

- As configurações de computador (configurações de política aplicadas a máquinas) definem o comportamento dos desktops virtuais e são aplicadas quando um desktop virtual é iniciado. Essas configurações são aplicadas mesmo quando não há sessões de usuário ativas no desktop virtual.
- As configurações de usuário definem a experiência do usuário ao se conectar usando ICA. As políticas de usuário são aplicadas quando um usuário se conecta ou reconecta usando ICA. As políticas de usuário não são aplicadas se um usuário se conecta usando RDP ou faz logon diretamente no console.

  Para acessar políticas, configurações ou modelos, selecione **Políticas** no painel esquerdo do Web Studio.

  - A guia **Políticas** lista todas as políticas. Ao selecionar uma política, as guias na parte inferior exibem:
    - Visão geral - Lista nome, prioridade, status ativado/desativado e descrição
    - Configurações - Lista todas as configurações configuradas
    - Atribuído a - Lista os objetos de usuário e máquina aos quais a política está atribuída. Para obter mais informações, consulte Criar políticas.
  - A guia **Modelos** lista os modelos fornecidos pela Citrix e os modelos personalizados que você criou. Ao selecionar um modelo, as guias na parte inferior exibem:
    - Descrição (por que você pode querer usar o modelo)
    - Configurações (lista de configurações configuradas). Para obter mais informações, consulte Modelos de política.
  - A guia **Comparação** permite comparar as configurações em uma política ou modelo com as configurações em outras políticas ou modelos. Por exemplo, você pode querer verificar os valores das configurações para garantir a conformidade com as melhores práticas. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

Para pesquisar uma configuração em uma política ou modelo:

a. Selecione a política ou o modelo.
b. Selecione **Editar política** ou **Editar modelo** na barra de ações.
c. Na página **Configurações**, digite o nome da configuração no campo de **pesquisa**:

   Você pode refinar sua pesquisa selecionando:

   - Uma versão específica do produto
   - Uma categoria (por exemplo, Largura de banda)
   - Palavras-chave no nome da configuração
   - A caixa de seleção **Exibir somente selecionados**
   - Para pesquisar apenas as configurações que foram adicionadas à política selecionada.

Para uma pesquisa não filtrada, selecione **Todas as Configurações**.

- Para pesquisar uma configuração dentro de uma política:

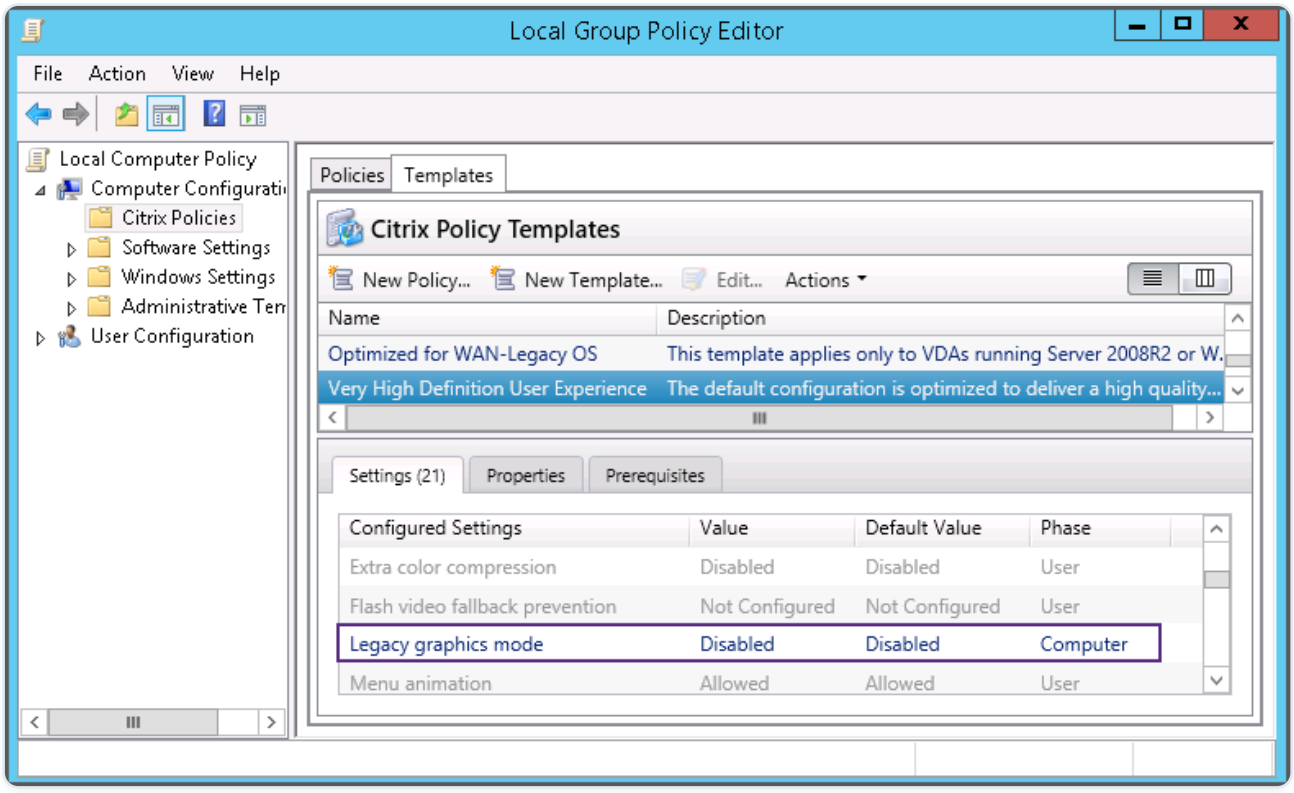
  a. Selecione a política.
  b. Selecione a guia **Configurações** e digite o nome da configuração.

Você pode refinar sua pesquisa selecionando uma versão específica do produto ou selecionando uma categoria. Para uma pesquisa não filtrada, selecione **Todas as Configurações**.

Uma política, uma vez criada, é independente do modelo usado. Você pode usar o campo **Descrição** em uma nova política para rastrear o modelo de origem usado.

No Editor de Política de Grupo, as configurações de computador e usuário devem ser aplicadas separadamente, mesmo que criadas a partir de um modelo que inclua ambos os tipos de configurações. Neste exemplo, a escolha de usar a Experiência de Usuário de Altíssima Definição na Configuração do Computador:

- O modo Gráficos Legados é uma configuração de Computador que é usada em uma política criada a partir deste modelo.
- As configurações de usuário, esmaecidas, não são usadas em uma política criada a partir deste modelo.




# Modelos de política

**Nota:**

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

Modelos são coleções de configurações que são recomendadas para serem usadas na criação de políticas para alcançar resultados específicos. Por exemplo, para criar políticas para fornecer uma experiência de usuário de alta definição aos usuários finais, as configurações definidas no modelo Experiência de Usuário de Altíssima Definição podem ser usadas como referência e ponto de partida para a criação de tais políticas.

Modelos não são políticas. Modelos são documentação suplementar para as configurações de política do Citrix. Eles demonstram as funcionalidades coletivas de certas configurações relacionadas ao usuário.

O uso de modelos é opcional. Os administradores podem criar políticas sem usar modelos. Os modelos são úteis para administradores que têm uma ideia de alto nível sobre como um site deve ser configurado, mas não têm certeza de quais configurações usar para alcançar a configuração desejada.

Os administradores podem criar os modelos usando um modelo existente, uma política existente ou do zero.

## ADMX/ADML

Os modelos de política de grupo do Citrix descritos aqui não têm nada a ver com os modelos de política do Windows. Os modelos descritos aqui e os modelos de política do Windows são dois conceitos diferentes. Os modelos de política de grupo do Citrix não são arquivos ADMX.

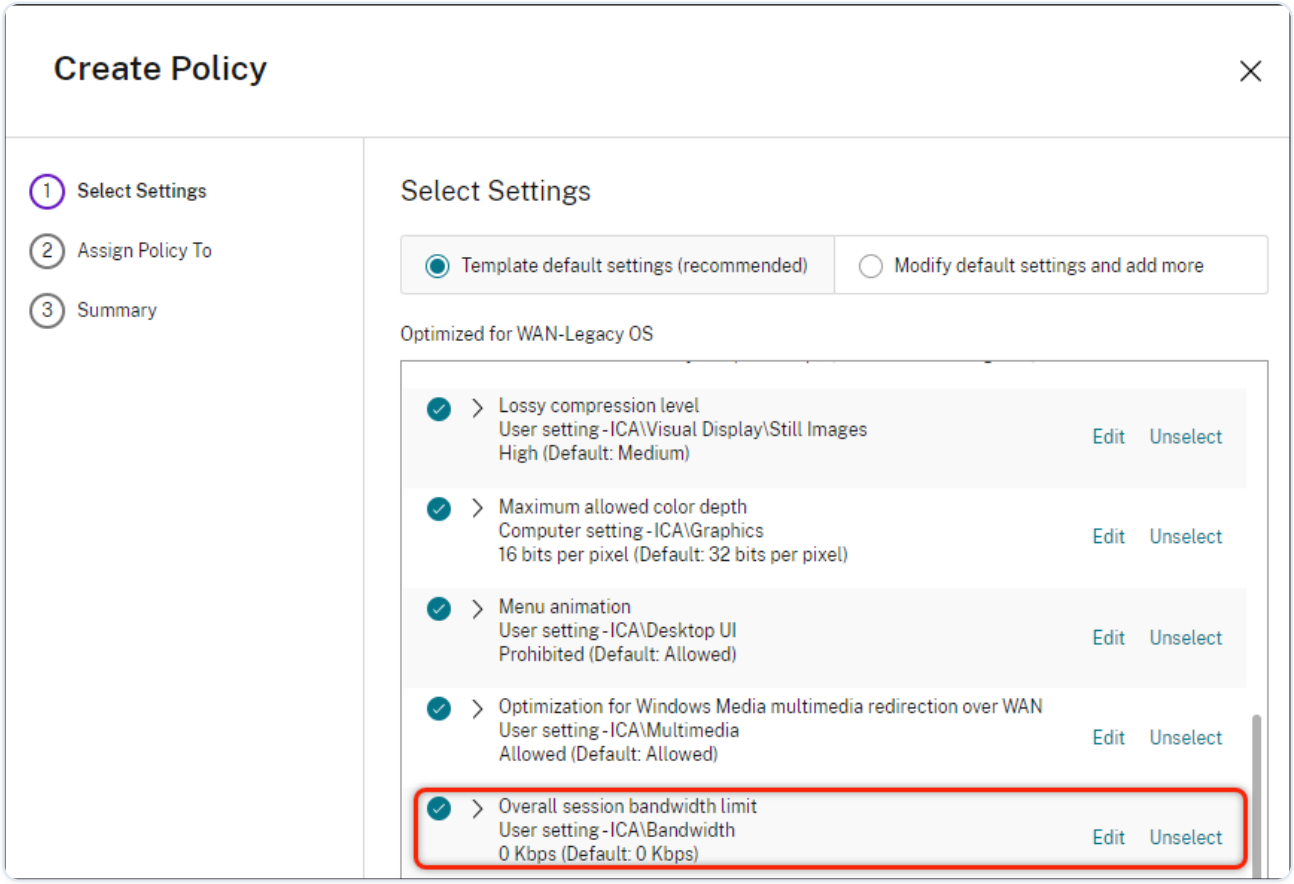
## Modelos Citrix integrados

Os seguintes modelos de política estão disponíveis:

- **Experiência de Usuário de Altíssima Definição**. Este modelo aplica configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde múltiplas políticas são processadas em ordem de precedência.
- **Alta Escalabilidade de Servidor**. Aplique este modelo para economizar recursos do servidor. Este modelo equilibra a experiência do usuário e a escalabilidade do servidor. Ele oferece uma boa experiência do usuário enquanto aumenta o número de usuários que você pode hospedar em um único servidor. Este modelo não usa um codec de vídeo para compressão de gráficos e impede a renderização multimídia do lado do servidor.
- **Alta Escalabilidade de Servidor - SO Legado**. Este modelo de Alta Escalabilidade de Servidor se aplica apenas a VDAs executando Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo depende do modo gráfico Legado, que é mais eficiente para esses sistemas operacionais.
- **Otimizado para NetScaler SD-WAN.** Aplique este modelo para usuários que trabalham em filiais com NetScaler SD-WAN para otimizar a entrega de Citrix Virtual Desktops. (NetScaler SD-WAN é o novo nome para CloudBridge).
- **Otimizado para WAN**. Este modelo é destinado a trabalhadores de tarefas em filiais que usam uma conexão WAN compartilhada ou locais remotos com conexões de baixa largura de banda acessando aplicativos com interfaces de usuário graficamente simples e pouco conteúdo multimídia. Este modelo troca a experiência de reprodução de vídeo e alguma escalabilidade do servidor por uma eficiência de largura de banda otimizada.

- **Otimizado para WAN-SO Legado**. Este modelo *Otimizado para WAN* aplica-se apenas a VDAs que executam Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo depende do modo gráfico Legado, que é mais eficiente para esses sistemas operacionais.
- **Segurança e Controle**. Use este modelo em ambientes com baixa tolerância a riscos, para minimizar os recursos habilitados por padrão no Citrix Virtual Apps and Desktops. Este modelo inclui configurações que desabilitam o acesso à impressão, área de transferência, dispositivos periféricos, mapeamento de unidades, redirecionamento de porta e aceleração Flash em dispositivos de usuário. A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade de usuários por servidor.

Embora recomendemos o uso dos modelos Citrix integrados com suas configurações padrão, existem configurações que não possuem um valor recomendado específico. Por exemplo, **Limite geral de largura de banda da sessão**, incluído nos modelos Otimizado para WAN. Neste caso, o modelo expõe a configuração para que o administrador entenda que esta configuração provavelmente se aplica ao cenário.




Se você estiver trabalhando com uma implantação (gerenciamento de políticas e VDAs) anterior ao XenApp e XenDesktop 7.6 FP3, e precisar dos modelos Alta Escalabilidade de Servidor e Otimizado para WAN, use as versões de SO Legado desses modelos quando aplicável.

**Nota:**

> A Citrix cria e atualiza modelos integrados. Você não pode modificar ou excluir esses modelos.

## Criar e gerenciar modelos usando o Web Studio

Para criar um modelo com base em um modelo:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e, em seguida, selecione o modelo a partir do qual você criará o modelo.
3. Selecione a guia **Criar Modelo**. A tela **Selecionar Configurações** é exibida.
4. Selecione e configure as configurações de política a serem incluídas no modelo.
5. Clique em **Avançar**. A tela **Resumo** é exibida.
6. Insira um nome para o modelo.
7. Clique em **Concluir**. O novo modelo aparece na guia **Modelos**.

Para criar um modelo com base em uma política:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Políticas** e, em seguida, selecione a política a partir da qual você cria o modelo.
3. Clique na guia **Mais**.
4. Selecione **Salvar como Modelo**. A tela **Selecionar Configurações** é exibida.
5. Selecione e configure quaisquer novas configurações de política a serem incluídas no modelo.
6. Clique em **Avançar**. A tela **Resumo** é exibida.
7. Insira um nome e uma descrição para o modelo e, em seguida, clique em **Concluir**.

## Modelos e administração delegada

Os modelos no Web Studio são armazenados no banco de dados do site, ao contrário dos modelos no Citrix Studio, que são armazenados como arquivos na pasta de perfil de usuário do administrador atual com uma extensão `.gpt`. Os modelos do Citrix Studio criados por um administrador não são visíveis para outros administradores ou para o mesmo administrador em uma máquina diferente. Os modelos do Web Studio são visíveis para todos os administradores sujeitos a permissões e administração delegada.

# Criar políticas

**Nota:**

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

Antes de criar uma política, decida qual grupo de usuários ou dispositivos ela pode afetar. Você pode querer criar uma política baseada na função de trabalho do usuário, tipo de conexão, dispositivo do usuário ou localização geográfica. Você também pode usar os mesmos critérios que usa para as políticas de grupo do Windows Active Directory.

Se você já criou uma política que se aplica a um grupo, considere editar essa política em vez de criar outra. Após editar a política, configure as definições apropriadas. Evite criar uma política apenas para habilitar uma configuração específica ou para excluir a política de se aplicar a determinados usuários.

Ao criar uma política, você pode baseá-la em configurações de um modelo de política e personalizar as configurações conforme necessário. Você também pode criá-la sem usar um modelo e adicionar todas as configurações de que precisa.

No Web Studio, as novas políticas criadas são definidas como Desabilitadas, a menos que a caixa de seleção **Habilitar política** seja explicitamente marcada.

Durante a criação da política e ao configurar as definições, o sistema oferece uma opção para visualizar o tipo de definição. Você pode visualizar os seguintes tipos de definição:

- Todas as configurações - Visualizar todas as aplicáveis a todas as versões do VDA
- Somente configurações atuais - Visualizar configurações específicas da versão atual do VDA
- Somente configurações herdadas - Visualizar configurações aplicáveis apenas às versões VDA descontinuadas

Para visualizar as configurações enquanto as configura:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Na guia **Políticas**, clique em **Criar Política**.

3. Na tabela **Selecionar Configurações**, clique no menu suspenso ao lado de **Configurações**.
4. Selecione uma das seguintes opções no menu suspenso:

- Todas as configurações - Visualizar todas as configurações para todas as versões do VDA
- Somente configurações atuais - Exibir configurações apenas para as versões atuais do VDA
- Somente configurações herdadas - Exibir configurações apenas para as versões VDA obsoletas

1. A tabela **Configurações** lista as configurações disponíveis com base na etapa anterior.

## Configurações de política

As configurações de política podem ser habilitadas, desabilitadas ou não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que elas não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

Algumas configurações de política podem estar em um dos seguintes estados:

- Permitido ou Proibido permite ou impede a ação controlada pela configuração. Às vezes, os usuários são permitidos ou impedidos de gerenciar a ação da configuração em uma sessão. Por exemplo, se a configuração de animação de menu for definida como Permitido, os usuários poderão controlar as animações de menu em seu ambiente de cliente.
- Habilitado ou Desabilitado ativa ou desativa a configuração. Se você desabilitar uma configuração, ela não será habilitada em políticas de classificação inferior.

Além disso, algumas configurações controlam a eficácia de configurações dependentes. Por exemplo, o redirecionamento de unidade de cliente controla se os usuários têm permissão para acessar as unidades em seus dispositivos. Tanto esta configuração quanto a configuração **Unidades de rede do cliente** devem ser adicionadas à política para permitir que os usuários acessem suas unidades de rede. Se a configuração **Redirecionamento de unidade de cliente** estiver desabilitada, os usuários não poderão acessar suas unidades de rede, mesmo que a configuração **Unidades de rede do cliente** esteja habilitada.

Em geral, as alterações nas configurações de política que afetam as máquinas entram em vigor quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon. As alterações nas configurações de política que afetam os usuários entram em vigor na próxima vez que os usuários fazem logon. Se você estiver usando o Active Directory, as configurações de política serão atualizadas quando o Active Directory reavaliar as políticas em intervalos de 90 minutos. E as

configurações de política são aplicadas quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon.

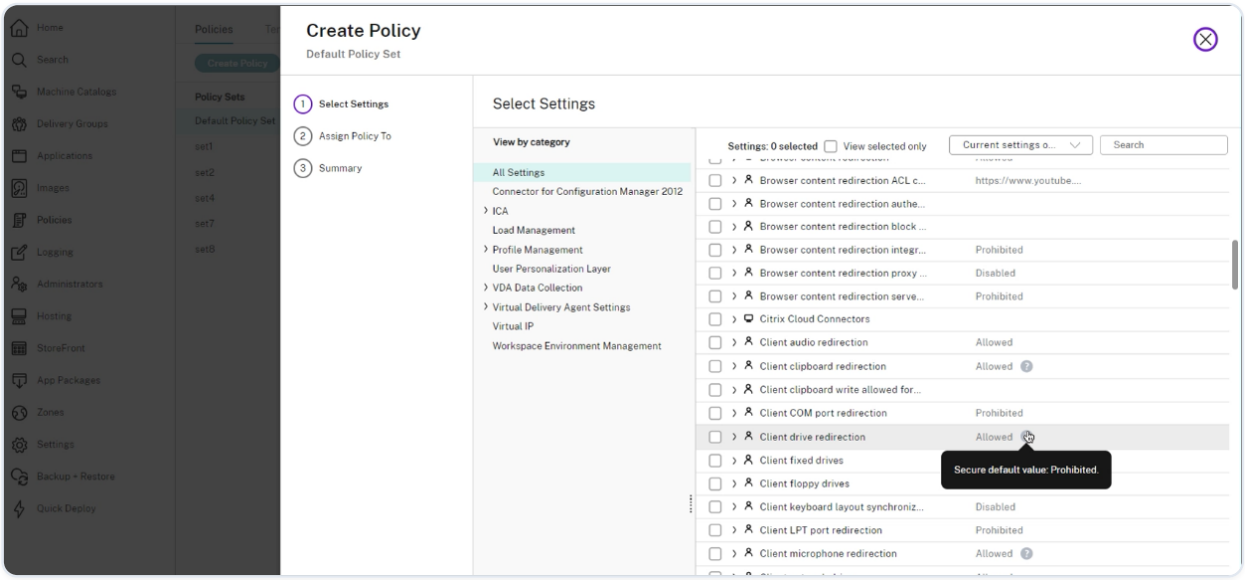
Para algumas configurações de política, você pode inserir ou selecionar um valor ao adicionar a configuração a uma política. Você pode limitar a configuração da configuração selecionando Usar valor padrão. Essa seleção desabilita a configuração da configuração e permite que apenas o valor padrão da configuração seja usado quando a política é aplicada. Essa seleção é independente do valor que foi inserido antes de selecionar Usar valor padrão.

Se a configuração padrão segura estiver habilitada, durante a instalação do VDA, a prioridade das configurações de política será afetada da seguinte forma:

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

Para ver a configuração padrão segura para uma política:

1. Faça logon no Web Studio.
2. Na navegação à esquerda, clique em **Políticas**.
3. Na guia **Políticas**, clique em **Criar Política**.
4. Na tabela **Selecionar Configurações**, quando você passa o mouse sobre as configurações que têm **Permitido?** como seu valor atual, o **Valor padrão seguro: Proibido** é exibido.




Como melhores práticas:

- Atribua políticas a grupos em vez de usuários individuais. Se você atribuir políticas a grupos, as atribuições serão atualizadas automaticamente quando você adicionar ou remover usuários do grupo.
- Não habilite configurações conflitantes ou sobrepostas na Configuração do Host da Sessão da Área de Trabalho Remota. Às vezes, a Configuração do Host da Sessão da Área de Trabalho Remota oferece funcionalidade semelhante às configurações de política do Citrix. Quando possível, mantenha todas as configurações consistentes (habilitadas ou desabilitadas) para facilitar a solução de problemas.
- Desative políticas não utilizadas. Políticas sem configurações adicionadas criam processamento desnecessário.

## Atribuições de política

Ao criar uma política, você a atribui a determinados usuários e objetos de máquina. Essa política é aplicada às conexões de acordo com critérios ou regras específicas. Em geral, você pode adicionar quantas atribuições quiser a uma política, com base em uma combinação de critérios.

Se você não especificar nenhuma atribuição, ou especificar atribuições mas desativá-las, a política será aplicada a **todas** as conexões.

> **Nota:**
>
> Atribuições de política também são conhecidas como filtros de política. Para obter informações adicionais, consulte os seguintes tópicos:
>
> - Criar, modificar ou excluir um filtro para uma política
> - Como os filtros são aplicados?

A tabela a seguir lista as atribuições disponíveis:

| NOME DA ATRIBUIÇÃO | APLICA UMA POLÍTICA COM BASE EM |
|---|---|
| Controle de Acesso | Condições de controle de acesso através das quais um cliente está se conectando. *Tipo de conexão* - Se a política deve ser aplicada a conexões feitas com ou sem o NetScaler® Gateway. *Nome do farm do NetScaler* |

| NOME DA ATRIBUIÇÃO | APLICA UMA POLÍTICA COM BASE EM |
|---|---|
| | *Gateway* - Nome do servidor virtual do NetScaler Gateway. *Condição de acesso* - Nome da política de análise de ponto de extremidade ou política de sessão a ser usada. |
| NetScaler SD-WAN | Se uma sessão de usuário é iniciada através do NetScaler SD-WAN. **Nota:** Você pode adicionar apenas uma atribuição de NetScaler SD-WAN a uma política. |
| Endereço IP do Cliente | Endereço IP do dispositivo do usuário usado para conectar-se à sessão: exemplos IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; exemplos IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Nome do Cliente | Nome do dispositivo do usuário. Correspondência exata: ClientABCName. Usando curinga: Client*Name. |
| Grupo de Entrega | Associação ao Grupo de Entrega. |
| Tipo de Grupo de Entrega | Tipo de área de trabalho ou aplicativo: área de trabalho privada, área de trabalho compartilhada, aplicativo privado ou aplicativo compartilhado. **Nota:** As opções de filtro de área de trabalho privada e área de trabalho compartilhada estão disponíveis apenas para Citrix Virtual Apps and Desktops 7.x. Para obter mais informações, consulte CTX219153. |
| Unidade Organizacional (OU) | Unidade organizacional. |
| Tag | Tags. **Nota:** Aplique esta política a todas as máquinas marcadas. As tags de aplicativo não estão incluídas. |
| Usuário ou Grupo | Nome do usuário ou grupo. |

Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas por ordem de prioridade e várias instâncias de qualquer configuração são comparadas. Cada configuração é aplicada de acordo com a classificação de prioridade da política. Qualquer configuração de política desabilitada tem precedência sobre uma configuração de classificação inferior que esteja habilitada. As configurações de política que não são configuradas são ignoradas.

> **Importante:**
>
> Ao configurar políticas do Active Directory e da Citrix usando o Console de Gerenciamento de Política de Grupo, as atribuições e configurações podem não ser aplicadas conforme o esperado. Para obter mais informações, consulte CTX127461
>
> Uma política chamada "Unfiltered" é fornecida por padrão.

- Se você usar o Web Studio para gerenciar políticas da Citrix, as configurações que você adicionar à política Unfiltered serão aplicadas a todos os servidores, desktops e conexões em um Site.
- Se você usar o Editor de Política de Grupo Local para gerenciar políticas da Citrix, as configurações que você adicionar à política Unfiltered serão aplicadas a todos os Sites e conexões. Os Sites e conexões devem estar dentro do escopo dos Objetos de Política de Grupo (GPOs) que incluem a política. Por exemplo, a UO de Vendas inclui um GPO chamado Sales-US que inclui todos os membros da equipe de vendas dos EUA. O GPO Sales-US é configurado com uma política Unfiltered que inclui várias configurações de política de usuário. Quando o gerente de vendas dos EUA faz logon no Site, as configurações da política Unfiltered são aplicadas automaticamente à sessão. Essa configuração ocorre porque o usuário é membro do GPO Sales-US.

O modo de uma atribuição determina se a política é aplicada apenas a conexões que correspondem a todos os critérios da atribuição. Se o modo for definido como Permitir (o padrão), a política será aplicada apenas a conexões que correspondem aos critérios da atribuição. Se o modo for definido como Negar, a política será aplicada se a conexão não corresponder aos critérios da atribuição. Os exemplos a seguir ilustram como os modos de atribuição afetam as políticas da Citrix quando várias atribuições estão presentes.

- **Exemplo: Atribuições do mesmo tipo com modos diferentes** - Em políticas com duas atribuições do mesmo tipo, uma definida como Permitir e outra como Negar, a atribuição

definida como Negar tem precedência, desde que a conexão satisfaça ambas as atribuições. Por exemplo:

A Política 1 inclui as seguintes atribuições:

- A Atribuição A especifica o grupo de Vendas. O modo é definido como Permitir.
- A Atribuição B especifica a conta do gerente de Vendas. O modo é definido como Negar.

Como o modo para a Atribuição B está definido como Negar, a política não é aplicada quando o gerente de Vendas faz logon no Site, mesmo que o usuário seja membro do grupo de Vendas.

- **Exemplo: Atribuições de tipos diferentes com modos semelhantes** - Em políticas com duas ou mais atribuições de tipos diferentes, definidas como Permitir, a conexão deve satisfazer pelo menos uma atribuição de cada tipo para que a política seja aplicada. Por exemplo:

  A Política 2 inclui as seguintes atribuições:

  - A Atribuição C é uma atribuição de Usuário que especifica o grupo de Vendas. O modo é definido como Permitir.
  - A Atribuição D é uma atribuição de Endereço IP do Cliente que especifica 10.8.169.* (a rede corporativa). O modo é definido como Permitir.

  Quando o gerente de Vendas faz logon no Site do escritório, a política é aplicada porque a conexão satisfaz ambas as atribuições.

  A Política 3 inclui as seguintes atribuições:

  - A Atribuição E é uma atribuição de Usuário que especifica o grupo Vendas. O modo está definido como Permitir.
  - A Atribuição F é uma atribuição de Controle de Acesso que especifica as condições de conexão do NetScaler Gateway. O modo está definido como Permitir.

  Quando o gerente de Vendas faz logon no Site do escritório, a política não é aplicada porque a conexão não satisfaz a Atribuição F.

## Criar uma política com base em um modelo, usando o Web Studio

1. Faça logon no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e selecione um modelo.
3. Selecione **Criar Política a partir do Modelo** na barra de ações.

4. Por padrão, a nova política usa todas as configurações padrão do modelo. Neste caso, **Configurações padrão do modelo (recomendado)** está selecionado. Se você quiser alterar as configurações, selecione **Modificar configurações padrão e adicionar mais** e, em seguida, adicione ou remova configurações.
5. Especifique como aplicar a política selecionando uma das seguintes opções:
   - **Objetos de usuário e máquina selecionados**. Para aplicar a política a objetos de usuário e máquina selecionados e, em seguida, clique em **Atribuir** para selecionar os objetos de usuário e máquina aos quais a política deve ser aplicada.
   - **Todos os objetos no site**. Para aplicar a política a todos os objetos de usuário e máquina no site.
6. Insira um nome para a política. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

   A política é desabilitada por padrão; você pode habilitá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem logon. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

## Criar uma política usando o Web Studio

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Políticas**.
3. Selecione **Criar Política** na barra de ações.
4. Adicione e configure as configurações da política.
5. Especifique como aplicar a política escolhendo uma das seguintes opções:
   - Atribua a objetos de usuário e máquina selecionados e, em seguida, selecione os objetos de usuário e máquina aos quais a política deve ser aplicada.
   - Atribua a todos os objetos em um site para aplicar a política a todos os objetos de usuário e máquina no Site.
6. Insira um nome para a política ou aceite o padrão. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

A política é habilitada por padrão; você pode desabilitá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem login. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

## Criar e gerenciar políticas usando o Editor de Política de Grupo

No Editor de Política de Grupo, expanda **Configuração do Computador ou Configuração do Usuário**. Expanda o nó **Políticas** e, em seguida, selecione **Políticas Citrix**. Escolha a ação apropriada:

| TAREFA | INSTRUÇÃO |
|---|---|
| Criar uma política | Na guia **Políticas**, clique em **Novo**. |
| Editar uma política existente | Na guia **Políticas**, selecione a política e, em seguida, clique em **Editar**. |
| Alterar a prioridade de uma política existente | Na guia **Políticas**, selecione a política e clique em **Superior** ou **Inferior**. |
| Exibir informações de resumo sobre uma política | Na guia **Políticas**, selecione a política e clique na guia **Resumo**. |
| Exibir e alterar configurações de política | Na guia **Políticas**, selecione a política e clique na guia **Configurações**. |
| Exibir e alterar filtros de política | Na guia **Políticas**, selecione a política e clique na guia **Filtros**. Ao adicionar mais de um filtro a uma política, todas as condições do filtro devem ser atendidas para que a política seja aplicada. |
| Habilitar ou desabilitar uma política | Na guia **Políticas**, selecione a política e selecione **Ações > Habilitar** ou **Ações > Desabilitar**. |
| Criar uma política a partir de um modelo existente | Na guia **Modelos**, selecione o modelo e clique em **Nova Política**. |

# Conjuntos de políticas

Conjuntos de políticas são objetos no Citrix Virtual Apps and Desktops™ que agregam políticas para permitir acesso simplificado baseado em função e fácil gerenciamento. Você pode criar conjuntos de políticas para espelhar divisões lógicas em sua equipe de administradores e empresa. Por exemplo, você pode criar um conjunto de políticas para cada região geográfica, unidade de negócios ou para um caso de uso específico. Uma vez criados, escopos e grupos de entrega são atribuídos a conjuntos de políticas para que apenas administradores autorizados possam gerenciar as políticas que se aplicam aos seus usuários e máquinas relevantes.

**Nota:**

Antes de habilitar os conjuntos de políticas, a Citrix® recomenda que você observe o seguinte:

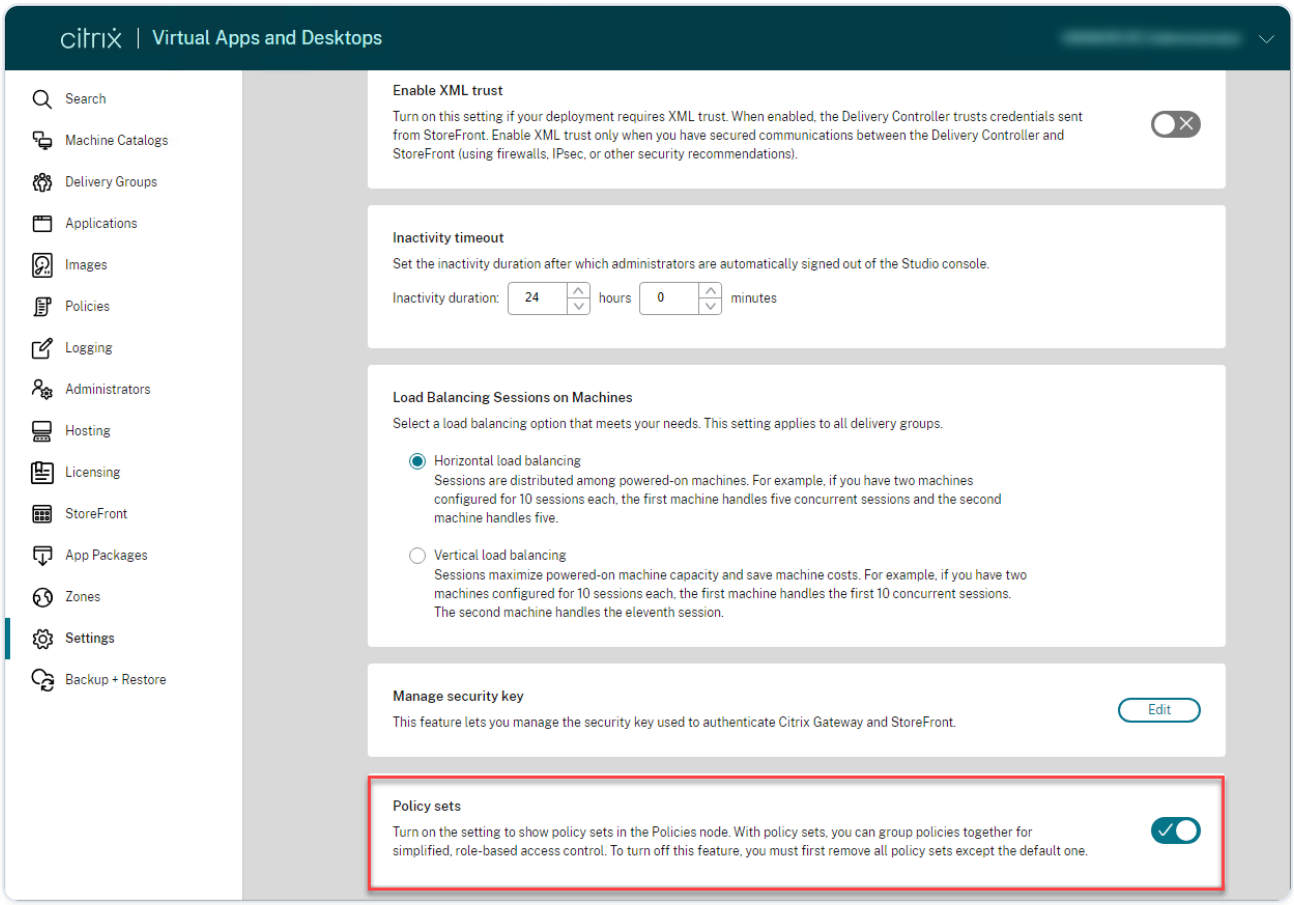
- Validações de política adicionais são adicionadas. Como resultado, fazer um upgrade no local pode levar à perda de dados de política se configurações de política inválidas estiverem presentes.
- Para detectar os dados inválidos, use a ferramenta de scanner GPO e faça as edições necessárias antes de atualizar. Para mais informações, consulte CTX676686.
- Para todas as futuras atualizações, a Citrix recomenda que você use o SDK mais recente. Usar um SDK mais antigo para atualizar políticas pode permitir a adição de dados inválidos às configurações de política, o que pode levar ao risco de perda de dados de política.

## Benefícios

- Controle de acesso baseado em função para equipes de administradores distribuídas
- Fusões, aquisições e consolidações simplificadas
- Domínio de falha limitado
- Suporte multilocatário para políticas

## Habilitar conjuntos de políticas

Na guia **Gerenciar** do Virtual Apps and Desktops, navegar até **Configurações** e ative a configuração **Conjuntos de políticas**.




**Nota:**

Você deve habilitar os conjuntos de políticas antes de criar um conjunto de políticas.

## Comparação de recursos

| ANTES DE APLICAR CONJUNTOS DE POLÍTICAS | DEPOIS DE APLICAR CONJUNTOS DE POLÍTICAS |
|---|---|
| Políticas, configurações, filtros e prioridades de política para todo o site são configurados em um só lugar no Citrix Studio. | Políticas, configurações, filtros e prioridades de política são configurados separadamente para cada conjunto de políticas. |
| Se você gerencia uma política, deve gerenciar todas as políticas. | Administradores completos podem delegar a administradores de nível inferior a capacidade de gerenciar um conjunto de políticas específico individualmente. |

| ANTES DE APLICAR CONJUNTOS DE POLÍTICAS | DEPOIS DE APLICAR CONJUNTOS DE POLÍTICAS |
| --- | --- |
| As políticas em ambientes grandes e distribuídos tornam-se complexas e difíceis de gerenciar. | As políticas em ambientes grandes e distribuídos podem ser divididas e gerenciadas facilmente. |

## Como funcionam os conjuntos de políticas?

### Visão geral

- Conjuntos de políticas são atribuídos a grupos de entrega
- Conjuntos de políticas têm um ou múltiplos escopos
- Grupos de entrega sem conjunto de políticas atribuído recebem o conjunto de políticas padrão
- Um grupo de entrega pode ter apenas um conjunto de políticas atribuído a ele
- Vários grupos de entrega podem usar o mesmo conjunto de políticas
- Embora os conjuntos de políticas sejam atribuídos a grupos de entrega, as políticas mantêm seus filtros

Para obter mais informações, consulte Como os filtros são aplicados?. Não há alteração na forma como as atribuições de política ou os filtros de política funcionam para conjuntos de políticas. Ou seja, eles funcionam da mesma forma que para as políticas.

### Conjunto de políticas padrão

- Quando a configuração do conjunto de políticas é ativada, todas as políticas existentes são agrupadas dentro do conjunto de políticas padrão
- Todo grupo de entrega recebe o conjunto de políticas padrão, a menos que a equipe de administradores crie um conjunto de políticas e o atribua a um grupo de entrega.
- Uma vez que um grupo de entrega tenha um conjunto de políticas diferente atribuído a ele, ele não receberá mais políticas do conjunto de políticas padrão

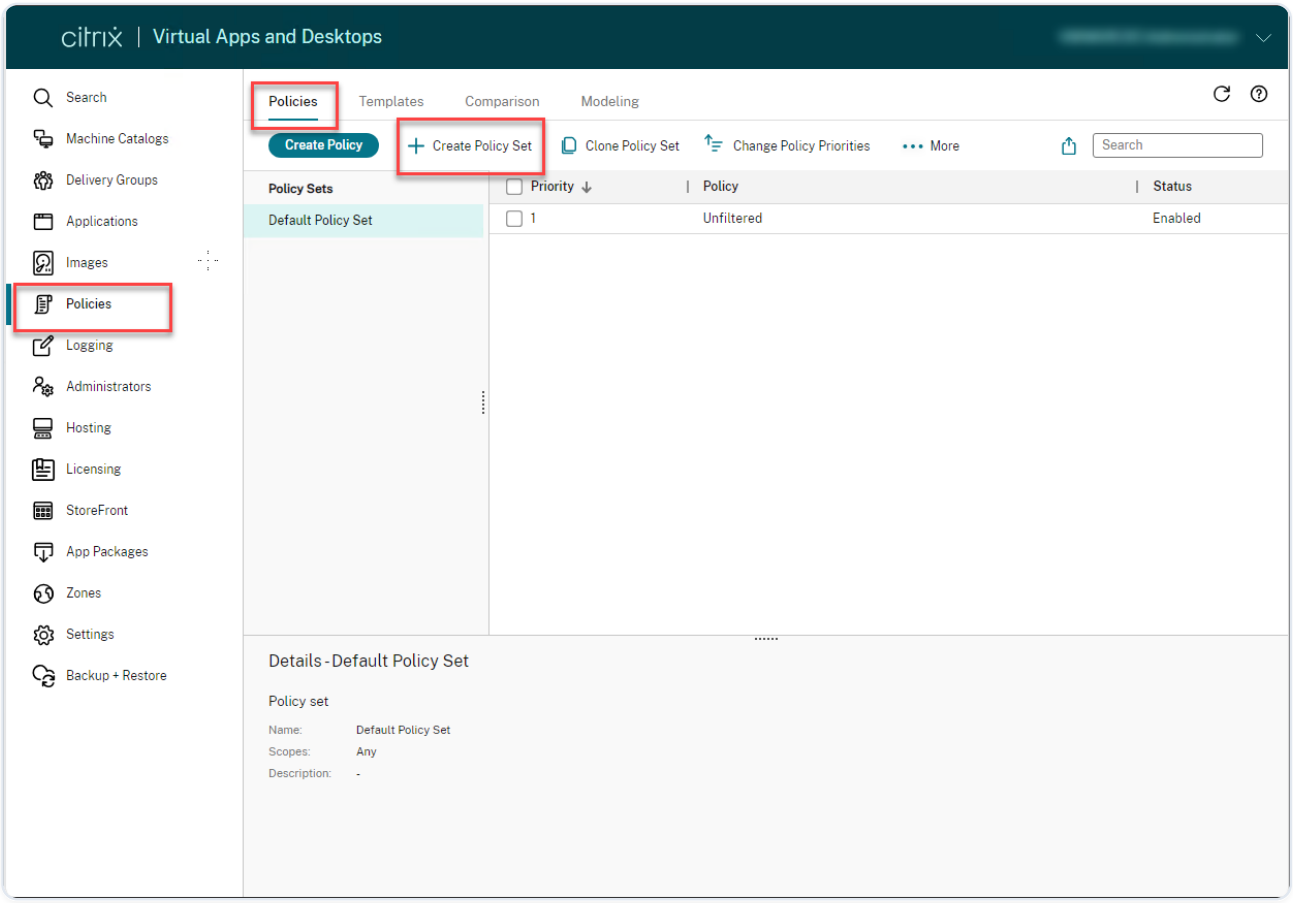
### Criação de conjunto de políticas

Os conjuntos de políticas podem ser criados das duas maneiras a seguir:

- Criar conjunto de políticas — esta ação cria um conjunto de políticas vazio
- Clonar conjunto de políticas — esta ação cria um conjunto de políticas com base em um conjunto de políticas existente

### Criar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.




1. Selecione **Criar Conjunto de Políticas**. A guia **Introdução** é exibida.
2. Clique em **Avançar** ou clique na guia **Nome e Descrição**.
3. Insira o nome e a descrição do conjunto de políticas.
4. Clique em **Avançar** ou clique na guia **Atribuições**.
5. Selecione um ou mais grupos de entrega aos quais você deseja atribuir o conjunto de políticas.
6. Clique em **Avançar** ou clique na guia **Escopos**.
7. Selecione os escopos do conjunto de políticas.
8. Clique em **Criar**. O conjunto de políticas é criado com a atribuição e o escopo definidos.

### Clonar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione **Clonar Conjunto de Políticas**.
3. Modifique o nome do conjunto de políticas.

4. Modifique ou crie atribuições para o conjunto de políticas e clique em **Avançar**.
5. Selecione ou desmarque as políticas a serem incluídas no conjunto de políticas clonado.
6. Modifique o escopo da política.
7. Clique em **Criar**. O conjunto de políticas é criado.

### Editar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione **Editar Conjunto de Políticas**.
3. Modifique o nome do conjunto de políticas e clique em **Avançar**.
4. Modifique ou crie atribuições para o conjunto de políticas e clique em **Avançar**.
5. Modifique o escopo da política.
6. Clique em **Criar**.

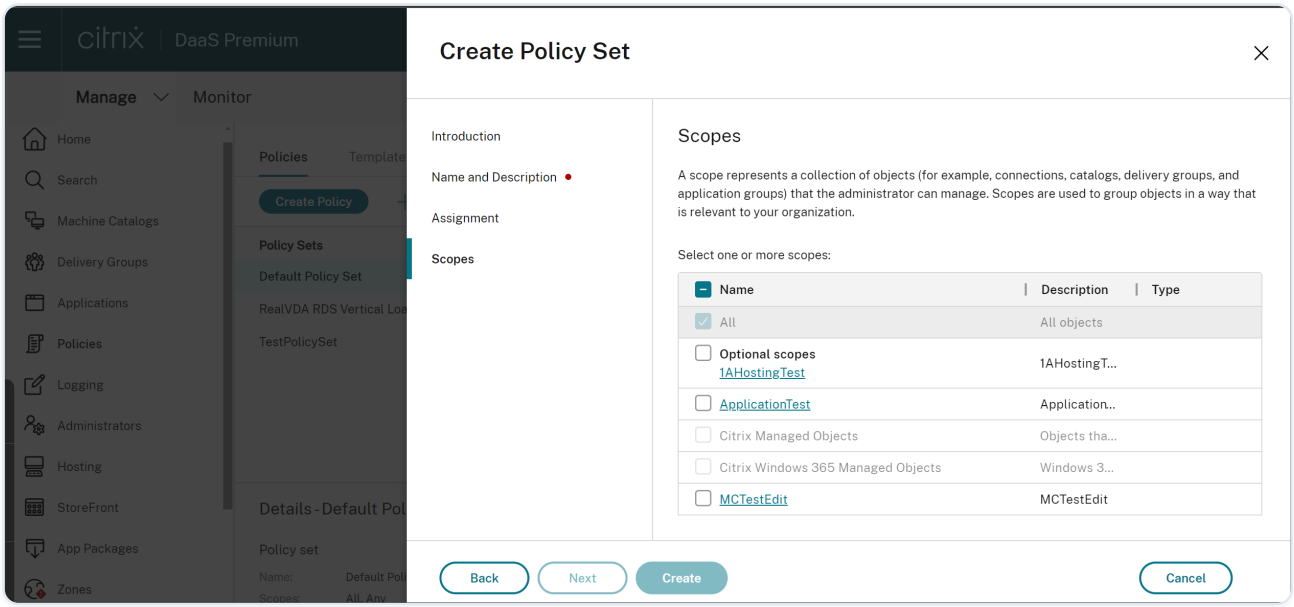
### Atribuição de conjunto de políticas

Os conjuntos de políticas são atribuídos a grupos de entrega. Você pode configurar atribuições quando o conjunto de políticas é criado ou editado. Você também pode configurar atribuições quando os grupos de entrega são criados ou editados.

### Escopos de conjunto de políticas

Os administradores podem definir o escopo do conjunto de políticas para que apenas administradores autorizados possam visualizá-lo ou editá-lo. Você pode configurar escopos quando o conjunto de políticas é criado ou editado.

Com a introdução dos Conjuntos de Políticas, você também pode criar e gerenciar a Política Citrix usando a API. Para obter mais informações, consulte Como criar um conjunto de políticas no Citrix DaaS.




# Comparar, priorizar e solucionar problemas de políticas

**Nota:**

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

Você pode usar várias políticas para personalizar seu ambiente para atender às necessidades dos usuários com base em suas funções de trabalho, localizações geográficas ou tipos de conexão. Por exemplo, para maior segurança, coloque restrições em grupos de usuários que interagem regularmente com dados confidenciais.

Você também pode criar uma política que impede os usuários de salvar arquivos confidenciais em suas unidades de cliente locais. No entanto, se alguns usuários no grupo de usuários precisarem de acesso às suas unidades locais, você poderá criar outra política apenas para esses usuários. Em seguida, você classifica ou prioriza as duas políticas para controlar qual delas tem precedência. Ao usar várias políticas, você deve determinar:

- Como priorizar as políticas
- Como criar exceções
- Como visualizar a política efetiva quando as políticas entram em conflito.

Em geral, as políticas substituem configurações semelhantes configuradas para todo o Site, para Delivery Controllers específicos ou no dispositivo do usuário. A exceção a esse princípio é a segurança. A configuração de criptografia mais alta em seu ambiente sempre substitui outras configurações e políticas. A configuração de criptografia mais alta inclui o sistema operacional e as configurações de sombreamento mais restritivas.

As políticas Citrix interagem com as políticas que você define em seu sistema operacional. Em um ambiente Citrix, as configurações Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou usando a Configuração do Host da Sessão da Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão de cliente do Protocolo de Área de Trabalho Remota (RDP). As configurações típicas de RDP incluem configurações como papel de parede da área de trabalho, animação de menu e visualização do conteúdo da janela ao arrastar.

Algumas configurações de política, como Secure ICA®, devem corresponder às configurações do sistema operacional. Se um nível de criptografia de prioridade mais alta for definido em outro lugar, as configurações da **política Secure ICA** que você especificar na política ou ao entregar aplicativos e desktops poderão ser substituídas.

Por exemplo, as configurações de criptografia que você especifica ao criar Delivery Groups devem estar no mesmo nível das configurações de criptografia que você especificou em todo o seu ambiente.

> **Nota:**
>
> No segundo salto de cenários de salto duplo, considere que um VDA de SO de sessão única se conecta a um VDA de SO de várias sessões. Nesse caso, as políticas Citrix atuam no VDA de SO de sessão única como se fosse o dispositivo do usuário. Por exemplo, considere que as políticas são definidas para armazenar imagens em cache no dispositivo do usuário. Neste exemplo, as imagens armazenadas em cache para o segundo salto em um cenário de salto duplo são armazenadas em cache na máquina VDA de SO de sessão única.

## Usar o assistente de modelagem de política

A modelagem de política ajuda você a simular políticas habilitadas com filtros para fins de planejamento e teste. Somente políticas habilitadas com filtros são modeladas. As políticas desabilitadas nunca são aplicadas e as políticas habilitadas sem filtros são sempre aplicadas.

Execute as seguintes etapas para abrir o assistente de **Modelagem de Políticas**:

1. Selecione **Políticas** na navegação à esquerda.
2. Selecione a guia **Modelagem**.
3. Selecione **Modelagem de Política** na barra de ações.
4. Leia a página **Introdução** e clique em **Avançar**.
5. Selecione usuários ou computadores. Você pode procurar por contêineres ou usuários ou computadores específicos. Clique em **Avançar**.
6. Escolha sua evidência de filtro. Opcionalmente, você pode ser mais granular com sua simulação inserindo detalhes adicionais, como **Grupo de entrega**, **Tags**, **Endereço IP do cliente** e assim por diante. Clique em **Avançar**.
7. Revise o resumo de suas seleções e clique em **Executar**.

Depois de clicar em **Executar**, o assistente gera um relatório dos resultados da modelagem. Ao visualizar este relatório, você pode:

- Selecione se deseja visualizar **Todas as configurações**, **Configurações do computador** ou **Configurações do usuário** no menu suspenso.
- Use a barra de pesquisa para procurar configurações específicas.
- Clique em uma configuração específica para ver os detalhes dessa configuração. Por exemplo, se todas as configurações de usuário não foram aplicadas para uma política específica, o painel **Detalhes** mostra o motivo pelo qual as configurações não foram aplicadas.
- Clique em **Exportar** para exportar os resultados da modelagem no formato JSON, formato HTML ou ambos.

Após executar a modelagem de políticas, mais opções ficam disponíveis para você. Você pode:

- **Exibir Relatório de Modelagem**: Isso abre o mesmo relatório de modelagem de cima para que você possa visualizá-lo novamente ou exportá-lo.
- **Executar Novamente a Modelagem de Política**: Isso permite que você execute novamente a modelagem de política com o mesmo conjunto de critérios selecionados anteriormente e gere novos resultados de modelagem. Isso é útil se algumas políticas foram alteradas e você gostaria de ver como essas alterações afetam seu modelo atual.
- **Excluir Relatório de Modelagem**: Isso exclui o relatório de modelagem atual.

## Comparar políticas e modelos

Você pode comparar as configurações em uma política ou modelo com as configurações de outras políticas ou modelos. Por exemplo, você pode precisar verificar os valores das configurações para manter a conformidade com as melhores práticas. Você também pode querer comparar as configurações em uma política ou modelo com as configurações padrão fornecidas pela Citrix.

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Clique na guia **Comparação** e, em seguida, clique em **Selecionar**.
3. Escolha as políticas ou modelos a serem comparados. Para incluir valores padrão na comparação, selecione a caixa de seleção **Comparar com as configurações padrão**.
4. Depois de clicar em **Comparar**, as configurações configuradas são exibidas em colunas.
5. Para ver todas as configurações, selecione **Mostrar Todas as Configurações**. Para retornar à exibição padrão, selecione **Mostrar Configurações Comuns**.

## Priorizar políticas

A priorização de políticas permite definir a precedência das políticas quando elas contêm configurações conflitantes. Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas em ordem de prioridade e várias instâncias de qualquer configuração são comparadas. Cada configuração é aplicada de acordo com a classificação de prioridade da política.

Você prioriza as políticas atribuindo-lhes diferentes números de prioridade. Por padrão, as novas políticas recebem a prioridade mais baixa. Se as configurações da política entrarem em conflito, uma política com prioridade mais alta (um número de prioridade 1 é o mais alto) substitui uma política com prioridade mais baixa. As configurações são mescladas de acordo com a prioridade e a condição da configuração. Por exemplo, se a configuração está desabilitada ou habilitada. Qualquer configuração desabilitada substitui uma configuração de classificação inferior que está habilitada. As configurações de política que não estão configuradas são ignoradas e não substituem as configurações de classificações inferiores.

1. Selecione **Políticas** no painel esquerdo. Certifique-se de selecionar a guia **Políticas**.
2. Na guia **Políticas**, selecione **Alterar Prioridades de Política** na barra de ações. A página **Alterar Prioridades de Política** é exibida.
3. Na lista de prioridades, use uma das seguintes maneiras para alterar a prioridade de uma política:
    - Arraste a política para a posição desejada.

- Para movê-lo para cima ou para baixo em uma posição, clique no ícone de seta Para Cima ou Para Baixo, respectivamente.
- Para movê-lo para o topo ou para a parte inferior da lista, clique no ícone de seta Para o Topo ou Para a Parte Inferior, respectivamente.
- Para alterar o número de prioridade, clique no ícone **Editar**, insira um número conforme necessário e, em seguida, clique em **Salvar**.

4. Clique em **Salvar**.

## Exceções

Ao criar políticas para grupos de usuários, dispositivos de usuário ou máquinas, você pode descobrir que alguns membros do grupo exigem exceções a algumas configurações de política. Você pode criar exceções por meio de:

- Criar uma política apenas para os membros do grupo que precisam das exceções e, em seguida, classificar a política com uma prioridade mais alta do que a política para o grupo inteiro
- Usar o modo Negar para uma atribuição adicionada à política

Uma atribuição com o modo definido como Negar aplica uma política apenas a conexões que não correspondem aos critérios de atribuição. Por exemplo, uma política inclui as seguintes atribuições:

- A Atribuição A é uma atribuição de endereço IP de cliente que especifica o intervalo 208.77.88.*. O modo está definido como Permitir
- A Atribuição B é uma atribuição de usuário que especifica uma conta de usuário específica. O modo está definido como Negar.

A política é aplicada a todos os usuários que fazem logon no Site com endereços IP no intervalo especificado na Atribuição A. No entanto, a política não é aplicada ao usuário que faz logon no Site com a conta de usuário especificada na Atribuição B.

## Determinar quais políticas se aplicam a uma conexão

Uma conexão pode não responder como esperado porque várias políticas se aplicam. Se uma política de prioridade mais alta se aplicar a uma conexão, ela poderá substituir as configurações que você configurou na política original. Você pode calcular o Conjunto Resultante de Política e determinar como as configurações finais da política são mescladas para uma conexão.

Você pode calcular o Conjunto Resultante de Política das seguintes maneiras:

- Use o Assistente de **Modelagem de Política de Grupo do Citrix** para simular um cenário de conexão e discernir como as políticas do Citrix podem ser aplicadas. Você pode especificar condições para um cenário de conexão, como:
  - Controlador de domínio
  - Usuários
  - Valores de evidência de atribuição de política do Citrix
  - Configurações de ambiente simulado, como conexão de rede lenta O relatório que o assistente produz lista as políticas Citrix que entram em vigor no cenário. Como você faz logon no Controller como um usuário de domínio, o assistente calcula os resultados usando as configurações de política de site e os Objetos de Política de Grupo (GPOs) do Active Directory.
- Use **Resultados da Política de Grupo** para produzir um relatório descrevendo as políticas Citrix em vigor para um determinado usuário e controlador. A ferramenta Resultados da Política de Grupo ajuda você a avaliar o estado atual dos GPOs em seu ambiente e gera um relatório. O relatório gerado descreve como esses objetos, incluindo as políticas Citrix, estão sendo aplicados atualmente a um usuário e controlador específicos.

Você pode iniciar o Assistente de Modelagem de Política de Grupo Citrix no Web Studio. Ou, você pode iniciar a ferramenta Resultados da Política de Grupo através do Console de Gerenciamento de Política de Grupo no Windows.

As configurações de política de site criadas usando o Web Studio não são incluídas no Conjunto Resultante de Política nos seguintes casos:

- Se você executar o Assistente de Modelagem de Política de Grupo Citrix a partir do Console de Gerenciamento de Política de Grupo
- Se você executar a ferramenta Resultados da Política de Grupo a partir do Console de Gerenciamento de Política de Grupo

Para verificar se você obtém o Conjunto Resultante de Política mais abrangente, o Citrix recomenda iniciar o assistente de Modelagem de Política de Grupo do Citrix a partir do Web Studio, a menos que você crie políticas usando apenas o Console de Gerenciamento de Política de Grupo.

### Solucionar problemas de políticas

Usuários, endereços IP e outros objetos atribuídos podem ter várias políticas aplicadas simultaneamente. Esse cenário pode resultar em conflitos onde uma política pode não se comportar como esperado. Ao executar o Assistente de Modelagem de Política de Grupo Citrix ou a ferramenta Resultados da Política de Grupo, você pode descobrir que nenhuma política é aplicada às conexões de usuário. Em tal cenário, as configurações de política não são aplicadas aos usuários que se conectam aos seus aplicativos e desktops sob condições que correspondem aos critérios de avaliação da política. Esta situação ocorre quando:

- Nenhuma política possui atribuições que correspondam aos critérios de avaliação da política.
- As políticas que correspondem à atribuição não têm nenhuma configuração definida.
- As políticas que correspondem à atribuição estão desabilitadas.

Se você deseja aplicar configurações de política às conexões que atendem aos critérios especificados, certifique-se de que:

- As políticas que você deseja aplicar a essas conexões estão habilitadas.
- As políticas que você deseja aplicar têm as configurações apropriadas configuradas.

## Configurações de política padrão

As tabelas a seguir listam as configurações de política, seus padrões e as versões do Virtual Delivery Agent (VDA) às quais se aplicam.

### ICA®

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Transporte adaptável | Desativado. Usar quando preferido | VDA 7.13–7.15; VDA 7.16 até o atual |
| Redirecionamento da área de transferência do cliente | Permitido | Todas as versões do VDA |
| Formatos permitidos para gravação na área de transferência do cliente | Nenhum formato especificado | VDA 7.6 até o atual |
| Inicializações de desktop | Proibido | VDA para SO multi-sessão 7 até o atual |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Número da porta do listener ICA | 1494 | Todas as versões do VDA |
| Inicialização de programas não publicados durante a conexão do cliente | Proibido | VDA para SO multi-sessão 7 até o atual |
| Limitar o tamanho da transferência da área de transferência do cliente para a sessão | Desabilitado | VDA 2009 |
| Limitar o tamanho da transferência da área de transferência da sessão para o cliente | Desabilitado | VDA 2009 |
| Modo tolerante a perdas | Permitido | VDA 2003. Observação: O modo de tolerância a perdas ainda não está disponível. Esta versão do VDA o suporta quando ele se torna disponível. |
| Limites de tolerância a perdas | Quando o modo tolerante a perdas estiver disponível: Perda de pacotes: 5%, Latência: 300 ms (RTT) | VDA 2003 até o atual |
| Protocolo Rendezvous | Desabilitado | Aplica-se apenas a sessões HDX estabelecidas através do Citrix Cloud. |
| Restringir gravação da área de transferência do cliente | Proibido | VDA 7.6 até o atual |
| Restringir gravação da área de transferência da sessão | Proibido | VDA 7.6 até o atual |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Formatos permitidos para gravação da área de transferência da sessão | Nenhum formato especificado | VDA 7.6 até o atual |
| Alternar modo tablet | Ativado | VDA 7.16 até o atual; para VDA 7.14 e 7.15 LTSR, configure esta definição usando o registro. |
| Lista de permissões de canal virtual | Ativado | VDA 2109 até o atual |

## ICA/Entrega do Adobe Flash/Redirecionamento do Flash

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Prevenção de fallback de vídeo Flash | Não configurado | VDA 7.6 FP3 até o atual |
| Erro de prevenção de fallback de vídeo Flash *.swf | VDA 7.6 FP3 até o atual | |

## ICA/Áudio

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Áudio Adaptável | Ativado | Aplica-se a sessões de SO de sessão única e SO de múltiplas sessões de VDAs usando Citrix Virtual Apps and Desktops™ 2109 ou posterior. |
| Áudio sobre transporte UDP em tempo real | Permitido | Todas as versões de VDA |
| Plug N Play de áudio | Permitido | VDA para SO de múltiplas sessões 7 até o atual |
| Qualidade do áudio | Alta - áudio de alta definição | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de áudio do cliente | Permitido | Todas as versões VDA |
| Redirecionamento de microfone do cliente | Permitido | Todas as versões VDA |
| Modo tolerante a perdas para áudio | Proibido | Versões VDA 2402 e superiores |

## ICA/Reconexão automática de cliente

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Reconexão automática do cliente | Permitido | Todas as versões VDA |
| Autenticação de reconexão automática do cliente | Não exigir autenticação | Todas as versões VDA |
| Registro de reconexão automática do cliente | Não registrar eventos de reconexão automática | Todas as versões VDA |
| Tempo limite de reconexão automática do cliente | 120 segundos | VDA 7.13 até o atual |
| Nível de transparência da interface do usuário de reconexão | 80% | VDA 7.13 até o atual |

## ICA/Largura de banda

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Limite de largura de banda de redirecionamento de áudio | 0 Kbps | Todas as versões do VDA |
| Porcentagem de limite de largura de banda de redirecionamento de áudio | 0 | Todas as versões do VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Limite de largura de banda de redirecionamento de dispositivo USB do cliente | 0 Kbps | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente | 0 | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Limite de largura de banda de redirecionamento da área de transferência | 0 Kbps | Todas as versões de VDA |
| Porcentagem de limite de largura de banda de redirecionamento da área de transferência | 0 | Todas as versões de VDA |
| Limite de largura de banda de redirecionamento de porta COM | 0 Kbps | Todas as versões de VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo |
| Porcentagem de limite de largura de banda de redirecionamento de porta COM | 0 | Todas as versões de VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo |
| Limite de largura de banda de redirecionamento de arquivo | 0 Kbps | Todas as versões de VDA |
| Porcentagem de limite de largura de banda de redirecionamento de arquivo | 0 | Todas as versões de VDA |
| Limite de largura de banda de aceleração multimídia HDX MediaStream | 0 Kbps | VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 e VDA para SO de sessão única 7 até o VDA atual para SO |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| | | multissessão e VDA para SO de sessão única |
| Porcentagem do limite de largura de banda da aceleração multimídia HDX MediaStream | 0 | VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Limite de largura de banda de redirecionamento de porta LPT | 0 Kbps | Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro |
| Porcentagem de limite de largura de banda de redirecionamento de porta LPT | 0 | Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro |
| Limite geral de largura de banda da sessão | 0 Kbps | Todas as versões do VDA |
| Limite de largura de banda de redirecionamento de impressora | 0 Kbps | Todas as versões do VDA |
| Porcentagem de limite de largura de banda de redirecionamento de impressora | 0 | Todas as versões do VDA |
| Limite de largura de banda de redirecionamento de dispositivo TWAIN | 0 Kbps | VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN | 0 | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## Redirecionamento de conteúdo ICA/bidirecional

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Permitir redirecionamento de conteúdo bidirecional | Proibido | VDA 7.13 até o atual |
| URLs permitidas a serem redirecionadas para o cliente | vazio | VDA 7.13 até o atual |
| URLs permitidas para serem redirecionadas para o VDA | vazio | VDA 7.13 até o atual |
| Configuração de redirecionamento de conteúdo bidirecional | Desabilitado | VDA 2311 até o atual |

## Redirecionamento de conteúdo ICA/navegador

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de conteúdo do navegador | Permitido | VDA 7.16 até o atual |
| Configuração de ACL de redirecionamento de conteúdo do navegador | `https://www.youtube.com/*` | VDA 7.16 até o atual |
| Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador | Proibido | VDA 2106 até o atual |
| Configuração de proxy de redirecionamento de conteúdo do navegador | vazio | VDA 7.16 até o atual |
| Autenticação de proxy web de busca do servidor de redirecionamento de conteúdo do navegador | Proibido | VDA 2012 até o atual |

## Sensores ICA/Cliente

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Permitir que aplicativos usem a localização física do dispositivo cliente | Proibido | VDA 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## ICA/UI de Desktop

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de Composição da Área de Trabalho | Desabilitado (7.6 FP3 até o atual); Habilitado (5.6 até 7.6 FP2) | VDA 5.6, VDA para SO de Sessão Única 7 até 7.15 |
| Qualidade gráfica do Redirecionamento de Composição da Área de Trabalho | Médio | VDA 5.6, VDA para SO de Sessão Única 7 até 7.15 |
| Papel de parede da área de trabalho | Permitido | Todas as versões do VDA |
| Animação de menu | Permitido | Todas as versões do VDA |
| Visualizar conteúdo da janela ao arrastar | Permitido | Todas as versões do VDA |

## ICA/Monitoramento do usuário final

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Cálculo de ida e volta do ICA | Ativado | Todas as versões do VDA |
| Intervalo de cálculo de ida e volta do ICA | 15 segundos | Todas as versões do VDA |
| Cálculos de ida e volta do ICA para conexões ociosas | Desabilitado | Todas as versões do VDA |

## ICA/Experiência de desktop aprimorada

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Experiência de Desktop Aprimorada | Permitido | VDA para SO multissessão 7 até o atual |

## ICA/Redirecionamento de arquivo

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Conectar automaticamente unidades cliente | Permitido | Todas as versões VDA |
| Redirecionamento de unidade cliente | Permitido | Todas as versões VDA |
| Unidades fixas do cliente | Permitido | Todas as versões VDA |
| Unidades de disquete do cliente | Permitido | Todas as versões VDA |
| Unidades de rede do cliente | Permitido | Todas as versões VDA |
| Unidades ópticas do cliente | Permitido | Todas as versões de VDA |
| Unidades removíveis do cliente | Permitido | Todas as versões de VDA |
| Redirecionamento do host para o cliente | Desabilitado | VDA para SO multiusuário 7 até o atual |
| Preservar letras de unidade do cliente | Desabilitado | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Acesso somente leitura à unidade do cliente | Desabilitado | VDA 5.5, 5.6 FP1, VDA para SO multiusuário 7 até o atual, VDA para SO de sessão única 7 até o atual |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de pasta especial | Permitido | Somente implantações do Web Interface; VDA para SO multiusuário 7 até o atual |
| Usar gravações assíncronas | Desabilitado | Todas as versões de VDA |

## ICA/Gráficos

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Permitir compressão visualmente sem perdas | Desabilitado | VDA 7.6 até o atual |
| Limite de memória de exibição | 65.536 Kb | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Preferência de degradação do modo de exibição | Degradar profundidade de cor primeiro | Todas as versões do VDA |
| Visualização dinâmica de janelas | Ativado | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Indicador de status gráfico | Desabilitado | VDA 7.16 até o atual |
| Cache de imagem | Ativado | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Modo gráfico legado | Desabilitado | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Profundidade máxima de cor permitida | 32 bits por pixel | Todas as versões do VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Notificar o usuário quando o modo de exibição for degradado | Desabilitado | VDA para SO multi-sessão 7 até o atual |
| Otimizar para carga de trabalho de gráficos 3D | Desabilitado | VDA 7.17 até o atual |
| Enfileiramento e descarte | Ativado | Todas as versões do VDA |
| Compartilhamento de tela | Desabilitado | VDA 2112 |
| Usar codec de vídeo para compressão | Usar codec de vídeo quando preferencial | VDA 7.6 FP3 até o atual |
| Usar codificação de hardware para codec de vídeo | Ativado | VDA 7.11 até o atual |

## ICA/Graphics/Caching

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Limite de cache persistente | 3.000.000 bps | VDA para SO multissessão 7 até o atual |

## ICA/Graphics/Framehawk

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Canal de exibição Framehawk | Desabilitado | VDA 7.6 FP2 até o atual |
| Intervalo de portas do canal de exibição Framehawk | 3224,3324 | VDA 7.6 FP2 até o atual |

## ICA/Manter ativo

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Tempo limite de manter ativo do ICA | 60 segundos | Todas as versões do VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Manter o ICA ativo | Não enviar mensagens de manutenção de atividade do ICA | Todas as versões de VDA |

## ICA/Teclado e IME

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Sincronização do Layout do Teclado do Cliente e Melhoria do IME | Desabilitado | Aplica-se apenas a 1912 LTSR CU2 e posterior. |
| Habilitar Mapeamento de Layout de Teclado Unicode | Proibido | Aplica-se apenas a 1912 LTSR CU2 e posterior. |
| Ocultar Caixa de Mensagem Pop-up de Troca de Layout de Teclado | Proibido | Aplica-se apenas a 1912 LTSR CU2 e posterior. |

## ICA/Acesso a Aplicativos Locais

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Permitir Acesso a Aplicativos Locais | Proibido | VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Lista de bloqueio de redirecionamento de URL | Nenhum site é especificado | VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Lista de permissão de redirecionamento de URL | Nenhum site é especificado | VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |

## Experiência ICA/Móvel

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Exibição automática do teclado | Proibido | VDA 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Iniciar área de trabalho otimizada para toque | Permitido | VDA 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual. Esta configuração está desabilitada e não está disponível para máquinas Windows 10 e Windows Server 2016. |
| Caixa de combinação remota | Proibido | VDA 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## ICA/Multimídia

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de vídeo HTML5 | Proibido | VDA 7.12 até o atual |
| Limitar a qualidade do vídeo | Não configurado | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Redirecionamento do Microsoft Teams | Permitido | VDA para SO multi-sessão 1906 até o atual, VDA para SO de sessão única 1906 até o atual. |
| Conferência multimídia | Permitido | Todas as versões do VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Otimização para redirecionamento multimídia do Windows Media sobre WAN | Permitido | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Usar GPU para otimizar o redirecionamento multimídia do Windows Media em WAN | Proibido | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Prevenção de fallback do Windows Media | Não configurado | VDA 7.6 FP3 até o atual |
| Busca de conteúdo do lado do cliente do Windows Media | Permitido | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Redirecionamento do Windows Media | Permitido | Todas as versões do VDA |
| Tamanho do buffer de redirecionamento do Windows Media | 5 segundos | VDA 5, 5.5, 5.6 FP1 até o atual |
| Uso do tamanho do buffer de redirecionamento do Windows Media | Desabilitado | VDA 5, 5.5, 5.6 FP1 até o atual |

## Conexões ICA/Multi-Stream

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Áudio via UDP | Permitido | VDA para SO Multi-sessão 7 até o atual |
| Intervalo de portas UDP de áudio | 16500, 16509 | VDA 5.5, 5.6 FP1, VDA para SO Multi-sessão 7 até o atual, VDA para SO de Sessão Única 7 até o atual |
| Política Multi-Porta | A porta primária (2598) tem Alta Prioridade | VDA 5.5, 5.6 FP1, VDA para SO Multi-sessão 7 até o |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| | | atual, VDA para SO de Sessão Única 7 até o atual |
| Configuração de computador Multi-Stream | Desabilitado | VDA 5.5, 5.6 FP1, VDA para SO Multi-sessão 7 até o atual, VDA para SO de Sessão Única 7 até o atual |
| Configuração de usuário Multi-Stream | Desabilitado | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Configuração de atribuição de fluxo de canal virtual Multi-Stream | Consulte Configuração de atribuição de canal virtual Multi-Stream para atribuições de fluxo padrão | VDA 2003 |

## Redirecionamento de ICA/Porta

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Conectar automaticamente portas COM do cliente | Desabilitado | Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro |
| Conectar automaticamente portas LPT do cliente | Desabilitado | Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro |
| Redirecionamento de porta COM do cliente | Proibido | Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro |
| Redirecionamento de porta LPT do cliente | Proibido | Todas as versões VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo |

## ICA/Impressão

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de impressora cliente | Permitido | Todas as versões VDA |
| Impressora predefinida | Definir a impressora predefinida para a impressora principal do cliente | Todas as versões VDA |
| Atribuições de impressora | A impressora atual do utilizador é usada como impressora predefinida para a sessão | Todas as versões VDA |
| Preferência de registo de eventos de criação automática de impressora | Registar erros e avisos | Todas as versões VDA |
| Impressoras de sessão | Nenhuma impressora é especificada | Todas as versões de VDA |
| Aguardar a criação das impressoras (desktop) | Desabilitado | Todas as versões de VDA |

## ICA/Impressão/Impressoras Cliente

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Criar impressoras cliente automaticamente | Criar todas as impressoras cliente automaticamente | Todas as versões de VDA |
| Criar impressora universal genérica automaticamente | Desabilitado | Todas as versões de VDA |
| Nomes de impressoras cliente | Nomes de impressoras padrão | VDA 5.6 |
| Conexões diretas a servidores de impressão | Ativado | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Mapeamento e compatibilidade de driver de impressora | Nenhuma regra é especificada | Todas as versões de VDA |
| Retenção de propriedades da impressora | Mantido no perfil somente se não salvo no cliente | Todas as versões de VDA |
| Impressoras cliente retidas e restauradas | Permitido | VDA 5, 5,5, 5.6 FP1 |

## ICA/Impressão/Drivers

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Instalação automática de drivers de impressora embutidos | Ativado | Todas as versões de VDA |
| Preferência de driver universal | EMF; XPS; PCL5c; PCL4; PS | Todas as versões de VDA |
| Uso do driver de impressão universal | Usar impressão universal somente se o driver solicitado não estiver disponível | Todas as versões do VDA |

## ICA/Impressão/Servidor de Impressão Universal

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Habilitar Servidor de Impressão Universal | Desabilitado | Todas as versões do VDA |
| Porta do fluxo de dados de impressão (CGP) do Servidor de Impressão Universal | 7229 | Todas as versões do VDA |
| Limite de largura de banda de entrada do fluxo de impressão do Servidor de Impressão Universal (kbps) | 0 | Todas as versões do VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Porta do serviço web (HTTP/SOAP) do Servidor de Impressão Universal | 8080 | Todas as versões do VDA |
| Servidores de Impressão Universal para balanceamento de carga | Versões VDA 7.9 até a atual | |
| Limite de servidor de impressão universal fora de serviço | 180 (segundos) | Versões VDA 7.9 até a atual |

## ICA/Impressão/Impressão Universal

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Modo de processamento EMF de impressão universal | Enviar diretamente para a impressora | Todas as versões VDA |
| Limite de compactação de imagem de impressão universal | Melhor qualidade (compactação sem perdas) | Todas as versões VDA |
| Padrões de otimização de impressão universal | Compactação de Imagem: Qualidade de imagem desejada = Qualidade padrão, Habilitar compactação pesada = False; Cache de Imagem e Fonte: Permitir cache de imagens incorporadas = True; Permitir que não administradores modifiquem essas configurações = False; | Todas as versões VDA |
| Preferência de visualização de impressão universal | Não usar visualização de impressão para impressoras universais genéricas ou criadas automaticamente | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Limite de qualidade de impressão universal | Sem limite | Todas as versões de VDA |

## ICA/Segurança

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Nível mínimo de criptografia SecureICA | Básico | VDA para SO multissessão 7 até o atual |

## ICA/Limites do Servidor

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Intervalo do temporizador de inatividade do servidor | 0 milissegundos | VDA para SO multissessão 7 até o atual |

## Limites de ICA/Sessão

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Temporizador de sessão desconectada | Desabilitado | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Temporizador de sessão desconectada do Acesso Remoto a PC | Desabilitado | VDA para SO de sessão única 7 até o atual |
| Intervalo do temporizador de sessão desconectada | 1.440 minutos | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Temporizador de conexão de sessão | Desabilitado | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Intervalo do temporizador de conexão de sessão | 1.440 minutos | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Temporizador de inatividade da sessão | Ativado | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |
| Intervalo do temporizador de inatividade da sessão | 1.440 minutos | VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual |

## ICA/Confiabilidade da Sessão

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Conexões de confiabilidade da sessão | Permitido | Todas as versões de VDA |
| Número da porta de confiabilidade da sessão | 2598 | Todas as versões de VDA |
| Tempo limite de confiabilidade da sessão | 180 segundos | Todas as versões de VDA |

## ICA/Controle de Fuso Horário

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Estimar hora local para clientes legados | Ativado | VDA para SO multissessão 7 até o atual |
| Restaurar fuso horário do SO de sessão única na desconexão ou logoff da sessão | Ativado | Versão atual do VDA |
| Usar hora local do cliente | Usar fuso horário do servidor | Todas as versões do VDA |

## Dispositivos ICA/TWAIN

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Redirecionamento de dispositivo TWAIN do cliente | Permitido | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Nível de compactação TWAIN | Médio | VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## Dispositivos ICA/USB

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Regras de otimização de dispositivo USB do cliente | Ativado (VDA 7.6 FP3 até o atual); Desativado (VDA 7.11 até o atual); Por padrão, nenhuma regra é especificada | VDA 7.6 FP3 até o atual |
| Redirecionamento de dispositivo USB do cliente | Proibido | Todas as versões de VDA |
| Regras de redirecionamento de dispositivo USB do cliente | Nenhuma regra especificada | Todas as versões de VDA |
| Redirecionamento de dispositivo USB Plug and Play do cliente | Permitido | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## ICA/Exibição Visual

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Profundidade de cor preferida para gráficos simples | 24 bits por pixel | VDA 7.6 FP3 até o atual |
| Taxa de quadros alvo | 30 quadros por segundo | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Qualidade visual | Médio | VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |

## ICA/Exibição Visual/Imagens em Movimento

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Qualidade mínima da imagem | Normal | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Compressão de imagem em movimento | Ativado | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Nível de compressão progressiva | Nenhum | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Valor limite de compressão progressiva | 2.147.483.647 Kbps | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Taxa de quadros mínima de destino | 10 qps | VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual |

**Nota:**

A política **Taxa de quadros mínima de destino** foi preterida.

## ICA/Exibição Visual/Imagens Estáticas

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Compressão extra de cores | Desabilitado | Todas as versões do VDA |
| Limite de compressão extra de cores | 8.192 Kbps | Todas as versões do VDA |
| Compressão pesada | Desabilitado | Todas as versões do VDA |
| Nível de compressão com perdas | Médio | Todas as versões do VDA |
| Valor limite de compressão com perdas | 2.147.483.647 Kbps | Todas as versões do VDA |

## ICA/WebSockets

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Conexões WebSockets | Proibido | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Número da porta WebSockets | 8008 | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Lista de servidores de origem confiáveis do WebSockets | O curinga, *, é usado para confiar em todos os URLs do Receiver para Web | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## Gerenciamento de Carga

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Tolerância de logon simultâneo | 2 | VDA para SO multi-sessão 7 até o atual |
| Uso da CPU | Desabilitado | VDA para SO multi-sessão 7 até o atual |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Prioridade de processo excluída do uso da CPU | Abaixo do Normal ou Baixo | VDA para SO multi-sessão 7 até o atual |
| Uso de disco | Desabilitado | VDA para SO multissessão 7 até o atual |
| Número máximo de sessões | 250 | VDA para SO multissessão 7 até o atual |
| Uso de memória | Desabilitado | VDA para SO multissessão 7 até o atual |
| Carga base de uso de memória | Carga zero: 768 MB | VDA para SO multissessão 7 até o atual |

## Gerenciamento de Perfil/Configurações avançadas

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Desabilitar configuração automática | Desabilitado | Todas as versões de VDA |
| Fazer logoff do usuário se um problema for encontrado | Desabilitado | Todas as versões de VDA |
| Número de tentativas ao acessar arquivos bloqueados | 5 | Todas as versões de VDA |
| Processar arquivos de cookie da Internet no logoff | Desabilitado | Todas as versões de VDA |

## Gerenciamento de Perfis/Configurações básicas

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Gravação ativa | Desabilitado | Todas as versões de VDA |
| Habilitar Gerenciamento de Perfis | Desabilitado | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Grupos excluídos | Desabilitado. Membros de todos os grupos de usuários são processados. | Todas as versões de VDA |
| Suporte a perfil offline | Desabilitado | Todas as versões de VDA |
| Caminho para o armazenamento de usuário | Windows | Todas as versões de VDA |
| Processar logons de administradores locais | Desabilitado | Todas as versões de VDA |
| Grupos processados | Desabilitado. Membros de todos os grupos de usuários são processados. | Todas as versões de VDA |

## Gerenciamento de Perfil/Configurações de Plataforma Cruzada

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Grupos de usuários de configurações de plataforma cruzada | Desabilitado. Todos os grupos de usuários especificados em Grupos processados são processados | Todas as versões de VDA |
| Habilitar configurações de plataforma cruzada | Desabilitado | Todas as versões de VDA |
| Caminho para definições de plataforma cruzada | Desabilitado. Nenhum caminho é especificado. | Todas as versões de VDA |
| Caminho para o armazenamento de configurações de plataforma cruzada | Desativado. Windows\PM_CM é usado. | Todas as versões de VDA |
| Fonte para criar configurações multiplataforma | Desabilitado | Todas as versões de VDA |

## Gerenciamento de Perfil/Sistema de Arquivos/Exclusões

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Lista de exclusão - diretórios | Desativado. Todas as pastas no perfil do usuário são sincronizadas. | Todas as versões de VDA |
| Lista de exclusão - arquivos | Desativado. Todos os arquivos no perfil do usuário são sincronizados. | Todas as versões de VDA |

## Gerenciamento de Perfil/Sistema de Arquivos/Sincronização

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Diretórios a sincronizar | Desativado. Apenas pastas não excluídas são sincronizadas. | Todas as versões de VDA |
| Arquivos para sincronizar | Desabilitado. Apenas arquivos não excluídos são sincronizados. | Todas as versões de VDA |
| Pastas para espelhar | Desabilitado. Nenhuma pasta é espelhada. | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Conceder acesso de administrador | Desabilitado | Todas as versões de VDA |
| Incluir nome de domínio | Desabilitado | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/AppData(Roaming)

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho do AppData(Roaming) | Desabilitado. Nenhuma localização é especificada. | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Configurações de redirecionamento para AppData(Roaming) | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho AppData(Roaming) | Todas as versões VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Contatos

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho dos Contatos | Desabilitado. Nenhum local é especificado. | Todas as versões VDA |
| Configurações de redirecionamento para Contatos | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Contatos** | Todas as versões VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Área de Trabalho

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho da Área de Trabalho | Desabilitado. Nenhum local é especificado. | Todas as versões VDA |
| Configurações de redirecionamento para Área de Trabalho | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho da Área de Trabalho** | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Documentos

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho de Documentos | Desabilitado. Nenhum local é especificado. | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Configurações de redirecionamento para Documentos | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Documentos** | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Downloads

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho de Downloads | Desabilitado. Nenhum local é especificado. | Todas as versões de VDA |
| Configurações de redirecionamento para Downloads | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Downloads** | Todas as versões de VDA |

## Gerenciamento de perfil/Redirecionamento de pasta/Favoritos

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho dos Favoritos | Desabilitado. Nenhuma localização é especificada. | Todas as versões de VDA |
| Configurações de redirecionamento para Favoritos | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Favoritos** | Todas as versões de VDA |

## Gerenciamento de perfil/Redirecionamento de pasta/Links

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho dos Links | Desabilitado. Nenhuma localização é especificada. | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Configurações de redirecionamento para Links | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Links** | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Música

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho da música | Desabilitado. Nenhuma localização é especificada. | Todas as versões VDA |
| Configurações de redirecionamento para Música | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho da Música** | Todas as versões VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Imagens

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho das imagens | Desabilitado. Nenhuma localização é especificada. | Todas as versões VDA |
| Configurações de redirecionamento para Imagens | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho das Imagens** | Todas as versões VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Jogos Salvos

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho de Jogos Salvos | Desabilitado. Nenhuma localização é especificada. | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Configurações de redirecionamento para Jogos Salvos | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Jogos Salvos** | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Pesquisas

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho de Pesquisas | Desabilitado. Nenhuma localização é especificada. | Todas as versões de VDA |
| Configurações de redirecionamento para Pesquisas | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Pesquisas** | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Menu Iniciar

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho do Menu Iniciar | Desativado. Nenhuma localização é especificada. | Todas as versões de VDA |
| Configurações de redirecionamento para o Menu Iniciar | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho do Menu Iniciar | Todas as versões de VDA |

## Gerenciamento de Perfil/Redirecionamento de Pasta/Vídeo

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho do vídeo | Desativado. Nenhuma localização é especificada. | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Configurações de redirecionamento para Vídeo | O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho do vídeo** | Todas as versões de VDA |

## Configurações de Gerenciamento de Perfil/Log

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Ações do Active Directory | Desabilitado | Todas as versões de VDA |
| Informações comuns | Desabilitado | Todas as versões de VDA |
| Avisos comuns | Desabilitado | Todas as versões de VDA |
| Habilitar registro em log | Desabilitado | Todas as versões de VDA |
| Ações do sistema de arquivos | Desabilitado | Todas as versões de VDA |
| Notificações do sistema de arquivos | Desabilitado | Todas as versões de VDA |
| Logoff | Desabilitado | Todas as versões de VDA |
| Logon | Desabilitado | Todas as versões de VDA |
| Tamanho máximo do arquivo de log | 1048576 | Todas as versões de VDA |
| Caminho para o arquivo de log | Desabilitado. Os arquivos de log são salvos no local padrão; %SystemRoot%\System32\Logfiles\UserProfileManager. | Todas as versões de VDA |
| Informações personalizadas do usuário | Desabilitado | Todas as versões de VDA |

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Valores da política no logon e logoff | Desabilitado | Todas as versões de VDA |
| Ações do Registro | Desabilitado | Todas as versões de VDA |
| Diferenças do Registro no logoff | Desabilitado | Todas as versões de VDA |

## Gerenciamento de perfil/Manipulação de perfil

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Atraso antes de excluir perfis em cache | 0 | Todas as versões de VDA |
| Excluir perfis armazenados em cache localmente no logoff | Desabilitado | Todas as versões de VDA |
| Tratamento de conflitos de perfil local | Usar perfil local | Todas as versões de VDA |
| Migração de perfis existentes | Local e roaming | Todas as versões de VDA |
| Caminho para o perfil de modelo | Desabilitado. Novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez. | Todas as versões de VDA |
| Perfil de modelo substitui perfil local | Desabilitado | Todas as versões de VDA |
| Perfil de modelo substitui perfil de roaming | Desabilitado | Todas as versões de VDA |
| Perfil de modelo usado como um perfil obrigatório Citrix® para todos os logons | Desabilitado | Todas as versões de VDA |

## Gerenciamento de Perfil/Registro

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Lista de exclusão | Desabilitado. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff. | Todas as versões de VDA |
| Lista de inclusão | Desabilitado. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff. | Todas as versões de VDA |

## Gerenciamento de Perfis/Perfis de usuário transmitidos por streaming

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Sempre armazenar em cache | Desabilitado | Todas as versões de VDA |
| Tamanho do cache sempre | 0 Mb | Todas as versões de VDA |
| Streaming de perfil | Desabilitado | Todas as versões de VDA |
| Grupos de perfil de usuário transmitidos por streaming | Desabilitado. Todos os perfis de usuário dentro de uma OU são processados normalmente. | Todas as versões de VDA |
| Tempo limite para arquivos de bloqueio de área pendentes (dias) | 1 dia | Todas as versões de VDA |

## Receiver

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Lista de contas do StoreFront™ | Nenhuma loja especificada | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |

## Camada de personalização do usuário

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Caminho do Repositório da Camada de Usuário | Desabilitado. Nenhum caminho especificado. | VDA 19.12 e versões posteriores |
| Tamanho da Camada de Usuário em GB | 10 GB. Uma camada de usuário é um disco de provisionamento dinâmico que se expande até o tamanho definido. As camadas de usuário nunca diminuem de tamanho. | VDA 19.12 ou versões posteriores |

## Agente de Entrega Virtual

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Máscara de rede IPv6 de registro do Controller | Nenhuma máscara de rede é especificada | VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Porta de registro do Controller | 80 | Todas as versões do VDA |
| SIDs do Controller | Nenhum SID é especificado | Todas as versões do VDA |
| Controladores | Nenhum controlador é especificado | Todas as versões do VDA |
| Habilitar atualização automática de controladores | Ativado | VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| Usar apenas o registro de controlador IPv6 | Desabilitado | VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual |
| GUID do site | Nenhum GUID é especificado | Todas as versões do VDA |

### Virtual Delivery Agent/HDX 3D Pro

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Habilitar sem perdas | Ativado | VDA 5.5, 5.6 FP1 |
| Configurações de qualidade do HDX 3D Pro | VDA 5.5, 5.6 FP1 | |

### Virtual Delivery Agent/Monitoramento

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Habilitar monitoramento de processo | Desabilitado | VDA 7.11 até o atual |
| Habilitar monitoramento de recursos | Ativado | VDA 7.11 até o atual |

### IP virtual

| NOME | CONFIGURAÇÃO PADRÃO | VDA |
|---|---|---|
| Suporte a loopback de IP virtual | Desabilitado | VDA 7.6 até o atual |
| Lista de programas de loopback virtual de IP virtual | Nenhum | VDA 7.6 até o atual |

## Referência de configurações de política

As políticas incluem configurações que são aplicadas quando a política é imposta. As descrições nesta seção também indicam se mais configurações são necessárias para habilitar um recurso ou se são semelhantes a uma configuração.

### Referência rápida

As tabelas a seguir listam as configurações que você pode configurar dentro de uma política. Encontre a tarefa que você deseja concluir na coluna da esquerda e, em seguida, localize a configuração correspondente na coluna da direita.

Uma lista completa de todas as configurações de política está disponível nos formatos .CHM (HTML Compilado) e .CSV. Esses arquivos estão disponíveis na pasta `\program files\citrix\grouppolicy` no servidor onde o broker (controlador de entrega) está instalado. Você também pode baixar a versão mais recente das configurações de política clicando aqui.

## Áudio

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controlar se o uso de vários dispositivos de áudio é permitido | Plug N Play de áudio |
| Controlar se a entrada de áudio de microfones no dispositivo do usuário é permitida | Redirecionamento de microfone do cliente |
| Controlar a qualidade do áudio no dispositivo do usuário | Qualidade do áudio |
| Controlar o mapeamento de áudio para os alto-falantes no dispositivo do usuário | Redirecionamento de áudio do cliente |

## Largura de banda para dispositivos de usuário

| PARA LIMITAR A LARGURA DE BANDA USADA PARA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Mapeamento de áudio do cliente | Limite de largura de banda de redirecionamento de áudio ou Porcentagem de limite de largura de banda de redirecionamento de áudio |
| Recortar e colar usando uma área de transferência local | Limite de largura de banda de redirecionamento da área de transferência ou Porcentagem de limite de largura de banda de redirecionamento da área de transferência |
| Acesso em uma sessão a unidades de cliente locais | Limite de largura de banda de redirecionamento de arquivo ou Porcentagem de limite de largura de banda de redirecionamento de arquivo |

| PARA LIMITAR A LARGURA DE BANDA USADA PARA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Aceleração Multimídia HDX™ MediaStream | Limite de largura de banda de aceleração multimídia HDX MediaStream ou Porcentagem de limite de largura de banda de aceleração multimídia HDX MediaStream |
| Sessão do cliente | Limite geral de largura de banda da sessão |
| Impressão | Limite de largura de banda de redirecionamento de impressora ou Porcentagem de limite de largura de banda de redirecionamento de impressora |
| Dispositivos TWAIN (como uma câmera ou scanner) | Limite de largura de banda de redirecionamento de dispositivo TWAIN ou Porcentagem de limite de largura de banda de redirecionamento de dispositivo TWAIN |
| Dispositivos USB | Limite de largura de banda de redirecionamento de dispositivo USB do cliente ou Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente |

## Redirecionamento de unidades de cliente e dispositivos de usuário

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controla se as unidades no dispositivo do usuário são conectadas quando os usuários fazem logon no servidor ou não | Conectar automaticamente unidades cliente |
| Controla a transferência de dados de recortar e colar entre o servidor e a área de transferência local | Redirecionamento da área de transferência do cliente |
| Controla como as unidades são mapeadas do dispositivo do usuário | Redirecionamento de unidade cliente |
| Controla se os discos rígidos locais dos usuários estão disponíveis em uma sessão | Unidades fixas do cliente e redirecionamento de unidade cliente |

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controla se as unidades de disquete locais dos usuários estão disponíveis em uma sessão | Unidades de disquete do cliente e redirecionamento de unidade cliente |
| Controla se as unidades de rede dos usuários estão disponíveis em uma sessão | Unidades de rede do cliente e redirecionamento de unidade cliente |
| Controla se as unidades de CD, DVD ou Blu-ray locais dos usuários estão disponíveis em uma sessão | Unidades ópticas do cliente e Redirecionamento de unidade do cliente |
| Controla se as unidades removíveis locais dos usuários estão disponíveis em uma sessão | Unidades removíveis do cliente e Redirecionamento de unidade do cliente |
| Controla se os dispositivos TWAIN dos usuários, como scanners e câmeras, estão disponíveis em uma sessão e controla a compactação das transferências de dados de imagem | Redirecionamento de dispositivo TWAIN do cliente; Redirecionamento de compactação TWAIN |
| Controla se os dispositivos USB estão disponíveis em uma sessão | Redirecionamento de dispositivo USB do cliente e Regras de redirecionamento de dispositivo USB do cliente |
| Melhora a velocidade de gravação e cópia de arquivos para um disco cliente em uma WAN | Usar gravações assíncronas |

## Redirecionamento de conteúdo

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controla se deve usar o redirecionamento de conteúdo do servidor para o dispositivo do usuário | Redirecionamento de host para cliente |

## UI do Desktop

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controla se o papel de parede da área de trabalho é usado nas sessões dos usuários ou não | Papel de parede da área de trabalho |
| Visualizar conteúdo da janela enquanto uma janela é arrastada | Visualizar conteúdo da janela ao arrastar |

## Gráficos e multimídia

**Importante:**

A política do Flash permanece apenas para permitir que clientes com VDAs mais antigos usem controladores mais recentes (por exemplo, controladores da versão 1912) e ainda usem o Flash. Esta versão do VDA não oferece suporte ao Flash.

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controlar o número máximo de quadros por segundo enviados para os dispositivos do usuário a partir de desktops virtuais | Taxa de quadros de destino |
| Controlar a qualidade visual das imagens exibidas no dispositivo do usuário | Qualidade visual |
| Controlar se os sites podem exibir conteúdo Flash quando acessados em sessões | Lista de URLs de busca de conteúdo do lado do servidor Flash; Lista de compatibilidade de URLs Flash; Configuração de política de prevenção de fallback de vídeo Flash; Erro de prevenção de fallback de vídeo Flash *.swf |
| Controlar a compactação de vídeo renderizado no servidor | Usar codec de vídeo para compactação; Usar codificação de hardware para codec de vídeo |

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controlar a entrega de conteúdo web multimídia HTML5 aos usuários | Redirecionamento de vídeo HTML5 |

## Priorizar o tráfego de rede Multi-Stream

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Especificar portas para tráfego ICA® em várias conexões e estabelecer prioridades de rede | Política de Multiportas |
| Habilitar suporte para conexões multi-stream entre servidores e dispositivos de usuário | Multi-Stream (configurações de computador e usuário) |

## Imprimir

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
|---|---|
| Controlar a criação de impressoras cliente no dispositivo do usuário | Criar automaticamente impressoras cliente e Redirecionamento de impressora cliente |
| Controlar o local onde as propriedades da impressora são armazenadas | Retenção de propriedades da impressora |
| Controlar se o cliente ou o servidor processa as solicitações de impressão | Conexões diretas a servidores de impressão |
| Controlar se os usuários podem acessar impressoras conectadas aos seus dispositivos de usuário | Redirecionamento de impressora cliente |
| Controlar a instalação de drivers nativos do Windows ao criar automaticamente impressoras cliente e de rede | Instalação automática de drivers de impressora incluídos |
| Controlar quando usar o Driver de Impressora Universal | Uso do driver de impressão universal |
| Escolher uma impressora com base nas informações da sessão de usuário roaming | Impressora padrão |

| PARA ESTA TAREFA | USE ESTA CONFIGURAÇÃO DE POLÍTICA |
| --- | --- |
| Balancear carga e definir limite de failover para Servidores de Impressão Universal | Servidores de Impressão Universais para balanceamento de carga; Limite de fora de serviço dos Servidores de Impressão Universais |

**Observação:**

As políticas não podem ser usadas para habilitar um protetor de tela em uma sessão de área de trabalho ou aplicativo. Para usuários que exigem protetores de tela, o protetor de tela pode ser implementado no dispositivo do usuário.

## Configurações de política do ICA®

**Observação:**

Esta página fornece descrições e valores de configuração suportados para as configurações de política do ICA. Para obter mais informações sobre como trabalhar com políticas, consulte a seção Trabalhar com políticas.

### Transporte adaptável

Esta configuração permite ou impede o transporte de dados via EDT como primário e via TCP como fallback.

Por padrão, o transporte adaptável está habilitado (**Preferencial**), e o EDT é usado quando possível, com fallback para TCP. Você pode alterar sua configuração conforme necessário:

- **Preferencial**. O transporte adaptável via EDT é usado quando possível, com fallback para TCP.
- **Modo de diagnóstico**. O EDT é forçado e o fallback para TCP é desabilitado. Recomendamos esta configuração apenas para solução de problemas.
- **Desativado**. O TCP é forçado e o EDT é desabilitado.

Para obter mais informações, consulte Transporte adaptável.

### Configuração de arrastar e soltar

Esta configuração permite ou impede o arrasto de arquivos entre o cliente e aplicativos ou desktops virtuais. Por padrão, a política de arrastar e soltar está desabilitada. Você pode habilitar esta política se necessário.

### Tempo limite de espera para inicialização de aplicativo

Esta configuração especifica o valor do tempo limite de espera em milissegundos para que uma sessão aguarde o início do primeiro aplicativo. Se o início do aplicativo exceder este período, a sessão será encerrada.

Você pode escolher o tempo padrão (10.000 milissegundos) ou especificar um número em milissegundos.

### Redirecionamento da área de transferência do cliente

Essa configuração permite ou impede que a área de transferência no dispositivo do usuário seja mapeada para a área de transferência no servidor.

Por padrão, o redirecionamento da área de transferência é permitido.

Para evitar a transferência de dados de copiar e colar entre uma sessão e a área de transferência local, selecione **Proibir**. Os usuários ainda podem copiar e colar dados entre aplicativos em execução nas sessões.

Depois de permitir esta configuração, configure a largura de banda máxima permitida que a área de transferência pode consumir em uma conexão de cliente. Use as configurações **Limite de largura de banda de redirecionamento da área de transferência** ou **Porcentagem do limite de largura de banda de redirecionamento da área de transferência**.

#### Formatos permitidos de gravação da área de transferência do cliente

Quando a configuração **Restringir gravação da área de transferência do cliente** está **Habilitada**, os dados da área de transferência do host não podem ser compartilhados com o endpoint do cliente. Você pode usar esta configuração para permitir que formatos de dados específicos sejam compartilhados com a área de transferência do endpoint do cliente. Para usar esta configuração, habilite-a e adicione os formatos específicos a serem permitidos.

Os seguintes formatos de área de transferência são definidos pelo sistema:

- CF_TEXT
- CF_BITMAP

- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Os seguintes formatos personalizados são predefinidos em XenApp e XenDesktop e Citrix Virtual Apps and Desktops™:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

O formato HTML está desabilitado por padrão. Para habilitar este recurso:

- Verifique se **Redirecionamento da área de transferência do cliente** está definido como **Permitido**.
- Verifique se **Restringir gravação da área de transferência do cliente** está definido como **Habilitado**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja que sejam suportados) em **Formatos permitidos para gravação da área de transferência do cliente**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos a serem registrados no sistema. Os nomes dos formatos diferenciam maiúsculas de minúsculas.

Essa configuração não se aplica se a política **Redirecionamento da área de transferência do cliente** estiver definida como **Proibido** ou se a política **Restringir gravação da área de transferência do cliente** estiver definida como **Desabilitado**.

> **Observação:**
>
> Habilitar o suporte à cópia da área de transferência no formato HTML (CF_HTML) copia quaisquer scripts da origem do conteúdo copiado para o destino. Verifique se você confia na origem antes de prosseguir com a cópia. Se você copiar conteúdo contendo scripts, eles estarão ativos somente se você salvar o arquivo de destino como um arquivo HTML e executá-lo.

**Limitar o tamanho da transferência do cliente da área de transferência para a sessão**

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de um endpoint cliente para uma sessão virtual durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, habilite a configuração **Limitar o tamanho da transferência da área de transferência do cliente para a sessão**. Em seguida, no campo **Limite de Tamanho**, insira um valor em kilobytes para definir o tamanho da transferência de dados entre a área de transferência local e uma sessão.

Por padrão, esta configuração está desabilitada e não há limite para transferências do cliente para a sessão.

### HDX™ Direct

O HDX Direct permite que o cliente estabeleça automaticamente uma conexão direta com o host da sessão quando a comunicação direta estiver disponível. As conexões são estabelecidas de forma segura usando criptografia em nível de rede.

### Modo HDX Direct

O HDX Direct pode ser usado para estabelecer conexões diretas com hosts de sessão para clientes internos e externos. Essa configuração determina se o HDX Direct está disponível apenas para clientes internos ou para clientes internos e externos.

Quando definido como somente **Interno**, o HDX Direct tenta estabelecer conexões diretas apenas para clientes na rede interna.

Quando definido como **Interno** e **externo**, o HDX Direct tenta estabelecer conexões diretas para clientes internos e externos.

Por padrão, o HDX Direct é configurado apenas para clientes internos.

### Intervalo de portas do HDX Direct

O intervalo de portas que são usadas pelo HDX Direct para conexões de usuários externos. Por padrão, o HDX Direct usa o intervalo de portas: 55000–55250.

### Limitar tamanho da transferência da área de transferência da sessão para o cliente

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de uma sessão virtual para um endpoint cliente durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, habilite a configuração **Limitar tamanho da transferência da área de transferência da sessão para o cliente**. Em seguida, no campo **Limite de Tamanho**, insira um valor em kilobytes para definir o tamanho da transferência de dados entre uma sessão e a área de transferência local.

Por padrão, esta configuração está desabilitada e não há limite para transferências de sessão para cliente.

### Restringir gravação da área de transferência do cliente

Se esta configuração estiver **Habilitada**, os dados da área de transferência do host não poderão ser compartilhados com o endpoint do cliente. Você pode permitir formatos específicos habilitando a configuração **Client clipboard write allowed formats**.

Por padrão, esta configuração está **Desabilitada**.

### Restringir gravação da área de transferência da sessão

Quando esta configuração estiver **Habilitada**, os dados da área de transferência do cliente não poderão ser compartilhados com os aplicativos da sessão. Você pode permitir formatos específicos habilitando a configuração **Session clipboard write allowed formats**.

Por padrão, esta configuração está **Desabilitada**.

### Formatos permitidos para gravação da área de transferência da sessão

Quando a configuração **Restrict session clipboard write** estiver **Habilitada**, os dados da área de transferência do cliente não poderão ser compartilhados com os aplicativos da sessão. Você pode usar esta configuração para permitir que formatos de dados específicos sejam compartilhados com a área de transferência da sessão.

Os seguintes formatos de área de transferência são definidos pelo sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT

- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Os seguintes formatos personalizados são predefinidos em XenApp e XenDesktop e Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

O formato HTML está desabilitado por padrão. Para habilitar este recurso:

- Verifique se **Redirecionamento da área de transferência do cliente** está definido como **Permitido**.
- Verifique se **Restringir gravação da área de transferência da sessão** está definido como **Habilitado**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja que sejam suportados) em **Formatos permitidos para gravação da área de transferência da sessão**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos a serem registrados no sistema. Os nomes dos formatos diferenciam maiúsculas de minúsculas.

Esta configuração não se aplica se a política de **Redirecionamento da área de transferência do cliente** estiver definida como **Proibido** ou a política de **Restringir gravação da área de transferência da sessão** estiver definida como **Desabilitado**.

> **Observação:**
>
> Habilitar o suporte à cópia da área de transferência no formato HTML (CF_HTML) copia quaisquer scripts da origem do conteúdo copiado para o destino. Verifique se você confia na origem antes de prosseguir com a cópia. Se você copiar conteúdo contendo scripts, eles estarão ativos apenas se você salvar o arquivo de destino como um arquivo HTML e executá-lo.

### Início da área de trabalho

Esta configuração permite ou impede conexões a uma sessão nesse VDA usando uma conexão ICA por usuários não administrativos em um grupo de Usuários de Acesso Direto do VDA.

Por padrão, usuários não administrativos não podem se conectar a essas sessões.

Essa configuração não afeta usuários não administrativos em um grupo de Usuários de Acesso Direto VDA que estão usando uma conexão RDP. Esses usuários podem se conectar ao VDA quando essa configuração está ativada ou desativada. Essa configuração não afeta usuários não administrativos que não estão em um grupo de Usuários de Acesso Direto VDA. Esses usuários não podem se conectar ao VDA quando essa configuração está ativada ou desativada.

### Redirecionamento FIDO2

Essa configuração ativa ou desativa o redirecionamento FIDO2. O redirecionamento FIDO2 permite que os usuários aproveitem os componentes FIDO2 do endpoint local em uma máquina virtual. Os usuários podem autenticar a sessão virtual por meio de chaves de segurança FIDO2 ou biometria integrada em dispositivos que possuem TPM 2.0 e Windows Hello.

Quando essa configuração está **Permitida**, os usuários podem fazer a autenticação FIDO2 usando os recursos do endpoint local. Por padrão, essa configuração é **Permitida**.

### Tempo limite de conexão do listener ICA

Essa configuração especifica o tempo máximo de espera para que uma conexão usando o protocolo ICA seja concluída.

Por padrão, o tempo máximo de espera é de 120.000 milissegundos, ou dois minutos.

### Número da porta do listener ICA

Essa configuração especifica o número da porta TCP/IP usado pelo protocolo ICA no servidor.

Por padrão, o número da porta é definido como 1494.

Os números de porta válidos devem estar no intervalo de 0 a 65535 e não devem entrar em conflito com outros números de porta bem conhecidos. Se você alterar o número da porta, reinicie o servidor para que o novo valor entre em vigor. Se você alterar o número da porta no servidor, também deverá alterá-lo em cada aplicativo ou plug-in do Citrix Workspace™ que se conecta ao servidor.

### Teclado e Editor de Método de Entrada (IME)

Essa configuração ativa ou desativa o seguinte:

- Sincronização dinâmica do layout do teclado
- Editor de Método de Entrada (IME)
- Mapeamento de layout de teclado Unicode
- Oculta ou mostra a mensagem da caixa de diálogo de notificação de troca de layout do teclado

1. No Web Studio, selecione **Teclado e IME**.
2. Selecione **Sincronização do layout do teclado do cliente e melhoria do IME** para controlar a sincronização dinâmica do layout do teclado e os recursos genéricos do Editor de Método de Entrada (IME) do cliente no VDA. Você pode configurar:

   **Desativado** - sincronização dinâmica do layout do teclado e Editor de Método de Entrada (IME) genérico do cliente.

   **Suportar sincronização dinâmica do layout do teclado do cliente** - habilita a sincronização dinâmica do layout do teclado.

   **Suportar sincronização dinâmica do layout do teclado do cliente e melhoria do IME** - habilita tanto a sincronização dinâmica do layout do teclado quanto o Editor de Método de Entrada (IME) genérico do cliente.
3. Selecione **Habilitar mapeamento de layout de teclado Unicode** para habilitar ou desabilitar o mapeamento de teclado Unicode.
4. Selecione **Ocultar caixa de mensagem pop-up de troca de layout do teclado** para controlar se uma mensagem aparece ou não, indicando que o layout do teclado está sincronizando quando o usuário altera o layout do teclado do cliente. Se você impedir que a mensagem apareça, os usuários devem esperar alguns momentos antes de digitar para evitar a entrada incorreta de caracteres.

Configurações padrão:

- **Sincronização do layout do teclado do cliente e melhoria do IME**
  - Desabilitado no Windows Server 2016 e Windows Server 2019.
  - Suporta sincronização dinâmica do layout do teclado do cliente e melhoria do IME no Windows Server 2012 e Windows 2010.
- **Desabilitar mapeamento de layout de teclado Unicode**
- **Mostrar caixa de mensagem pop-up de troca de layout do teclado**

Esta política substitui as configurações de registro listadas na seção **Descrição** das configurações de política.

### Atraso na inicialização do verificador de logoff

Esta configuração especifica a duração para atrasar a inicialização do verificador de logoff. Use esta política para definir o tempo (em segundos) que uma sessão de cliente aguarda antes de desconectar a sessão.

Esta configuração também aumenta o tempo que um usuário leva para fazer logoff do servidor.

### Modo tolerante a perdas

> **Importante:**
>
> - O recurso requer no mínimo o Citrix Workspace app 2002 para Windows. Esta versão do VDA o suporta quando ele se torna disponível.
> - O modo tolerante a perdas para gráficos não é suportado no Citrix Gateway ou no Citrix Gateway Service. Este modo está disponível apenas com conexões diretas.

> Esta configuração habilita ou desabilita o modo tolerante a perdas para gráficos.

Por padrão, o modo tolerante a perdas para gráficos é **Permitido**.

Quando permitido, o modo é ativado quando a perda de pacotes e a latência estão acima de um limite. Você pode definir os limites usando a política de limites tolerantes a perdas.

### Limites tolerantes a perdas

Quando o Modo tolerante a perdas está disponível, esta configuração especifica os limites das métricas de rede nos quais a sessão muda para o modo tolerante a perdas para gráficos.

Os limites padrão são:

- Perda de pacotes: 5%
- Latência: 300 ms (RTT)

Para mais informações, consulte modo tolerante a perdas.

### Modo tolerante a perdas para áudio

Essa configuração habilita ou desabilita o modo tolerante a perdas para áudio.

Quando habilitado, o áudio é enviado através do modo tolerante a perdas.

Por padrão, o modo tolerante a perdas para áudio é **Proibido**.

Para habilitar a política, edite o registro da política de modo tolerante a perdas para áudio para **Permitido**.

O transporte EDT é necessário para habilitar o modo tolerante a perdas para áudio.

### Protocolo Rendezvous

Essa configuração altera como as sessões HDX são proxy quando se usa o Citrix Gateway Service. Quando habilitado, o tráfego HDX não flui mais através do Citrix Cloud Connector. Em vez disso, o VDA estabelece uma conexão de saída diretamente com o Citrix Gateway Service (melhorando a escalabilidade do Cloud Connector).

> **Importante:**
>
> Um alternador de recursos no Citrix Cloud™ e uma configuração de política HDX controlam esse recurso. O alternador de recursos do Citrix Cloud é habilitado por padrão, enquanto a configuração HDX é desabilitada por padrão. A configuração HDX afeta apenas as sessões HDX estabelecidas através do Citrix Gateway Service. Essa configuração não afeta as sessões estabelecidas diretamente entre o cliente e o VDA ou através de um Citrix Gateway local.

> Para obter informações, consulte protocolo Rendezvous.

### Configuração de proxy Rendezvous

Essa configuração permite configurar um proxy explícito para uso com o protocolo Rendezvous. Se estiver usando um proxy transparente, essa configuração não precisa ser habilitada.

Por padrão, essa configuração está desabilitada.

Quando desabilitado, o VDA não roteia o tráfego de saída através de nenhum proxy não transparente ao tentar estabelecer uma conexão Rendezvous com o Gateway Service.

Quando ativado, o VDA tenta estabelecer uma conexão Rendezvous com o Gateway Service por meio do proxy definido nesta configuração.

O VDA suporta o uso de proxies HTTP e SOCKS5 para conexões Rendezvous. Para configurar o VDA para usar um proxy para a conexão Rendezvous, você deve habilitar essa configuração. Além disso, especifique o endereço do proxy ou o caminho para o arquivo PAC. Por exemplo:

- Endereço do proxy: `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path>/<filename>.pac`

  A versão 2103 do VDA é a versão mínima compatível para configuração de proxy com um arquivo PAC. Para obter mais informações sobre o esquema de arquivo PAC para proxies SOCKS5, consulte Configuração de proxy.

> **Observação:**
>
> Somente proxies SOCKS5 suportam transporte de dados via EDT. Para um proxy HTTP, use TCP como protocolo de transporte para ICA.
>
> Para obter mais informações, consulte protocolo Rendezvous.

### Inicialização de programas não publicados durante a conexão do cliente

Esta configuração especifica se deve permitir a inicialização de aplicativos iniciais via RDP no servidor.

Por padrão, a inicialização de aplicativos iniciais via RDP no servidor não é permitida.

### Configurações de política de alternância do modo tablet

A alternância do modo tablet otimiza a aparência e o comportamento de aplicativos da Store, aplicativos Win32 e o shell do Windows no VDA. Isso é feito alternando automaticamente a área de trabalho virtual para o modo Tablet ao conectar-se de dispositivos de pequeno formato, como telefones e tablets, ou qualquer dispositivo habilitado para toque.

Se esta política estiver desabilitada, o VDA estará no modo que o usuário o configurou e manterá o mesmo modo durante todo o tempo, independentemente do tipo de cliente.

## Configurações de política de reconexão automática do cliente

A seção **Reconexão Automática do Cliente** contém configurações de política para controlar a reconexão automática de sessões.

### Reconexão automática do cliente

Essa configuração permite ou impede a reconexão automática pelo mesmo cliente após uma conexão ter sido interrompida.

Para Citrix Receiver para Windows 4.7 e posterior e Citrix Workspace app 1808 e posterior, a reconexão automática do cliente usa apenas as configurações de política do Citrix Studio. As atualizações dessas políticas no Studio sincronizam a reconexão automática do cliente do servidor para o cliente. Com versões mais antigas do Citrix Receiver para Windows, para configurar a reconexão automática do cliente, use uma política do Studio e altere o registro ou o arquivo default.ica.

Permitir a reconexão automática do cliente permite que os usuários retomem o trabalho de onde foram interrompidos quando uma conexão foi quebrada. A reconexão automática detecta conexões quebradas e, em seguida, reconecta os usuários às suas sessões.

Se o cookie do Citrix Workspace™ app contendo a chave para o ID da sessão e as credenciais não for usado, a reconexão automática poderá resultar no início de uma nova sessão. Ou seja, em vez de reconectar a uma sessão existente. O cookie não é usado se tiver expirado. Por exemplo, o cookie pode expirar devido a um atraso na reconexão ou se as credenciais precisarem ser reinseridas. Se os usuários se desconectarem intencionalmente, a reconexão automática do cliente não será acionada.

Uma janela de sessão fica esmaecida quando uma reconexão está em andamento. Um cronômetro de contagem regressiva exibe o tempo restante antes que a sessão seja reconectada. Quando uma sessão expira, ela é desconectada.

Para sessões de aplicativos, quando a reconexão automática é permitida, um cronômetro de contagem regressiva aparece na área de notificação. Este cronômetro especifica o tempo restante antes que a sessão seja reconectada. O Citrix Workspace app tenta reconectar-se à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de usuário, quando a reconexão automática é permitida, o Citrix Workspace app tenta reconectar-se à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, este período é de dois minutos. Para alterar este período, edite a política.

Por padrão, a reconexão automática do cliente é permitida. Você pode desativá-la definindo a política como **Proibida**.

#### Autenticação de reconexão automática do cliente

Essa configuração especifica se a autenticação é necessária para reconexões automáticas do cliente.

Quando um usuário faz logon inicialmente, as credenciais são criptografadas, armazenadas na memória e um cookie é criado contendo a chave de criptografia. O cookie é enviado para o Citrix Workspace app. Quando essa configuração é configurada, os cookies não são usados. Em vez disso, uma caixa de diálogo é exibida para os usuários solicitando credenciais quando o Citrix Workspace app tenta reconectar-se automaticamente.

Por padrão, a autenticação não é necessária.

#### Registro de reconexão automática do cliente

Esta configuração habilita ou desabilita o registro de reconexões automáticas do cliente no log de eventos.

Quando o registro está habilitado, o Log do Sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Um site não fornece um log combinado de eventos de reconexão para todos os servidores.

Por padrão, o registro está desabilitado.

#### Tempo limite de reconexão automática do cliente

Por padrão, o tempo limite de reconexão automática do cliente é definido como 120 segundos, o valor máximo configurável para um tempo limite de reconexão automática do cliente é de 300 segundos. Use esta política para definir o valor do tempo limite.

#### Nível de transparência da interface do usuário de reconexão

Essa configuração permite especificar o nível de opacidade aplicado à janela da sessão do XenApp ou XenDesktop® durante o tempo de reconexão da confiabilidade da sessão.

Por padrão, a transparência da interface do usuário de reconexão é definida como 80%.

### Configurações de política de áudio

A seção **Áudio** inclui configurações de política que permitem que os dispositivos do usuário enviem e recebam áudio em sessões sem reduzir o desempenho.

### Áudio Adaptável

Esta configuração habilita ou desabilita o áudio adaptável. Ao habilitar esta política, as configurações de qualidade de áudio são ajustadas dinamicamente para fornecer a melhor experiência do usuário. Esta configuração se aplica a sessões de SO de sessão única e SO de múltiplas sessões de VDAs usando Citrix Virtual Apps and Desktops™ 2109 ou posterior.

Quando esta configuração é proibida, a política de qualidade de áudio é aplicada. Para obter mais informações, consulte Qualidade de áudio.

Por padrão, a política de áudio adaptável está habilitada.

### Áudio sobre transporte UDP em tempo real

Esta configuração permite ou impede a transmissão e o recebimento de áudio entre o VDA e o dispositivo do usuário via RTP usando o User Datagram Protocol (UDP). Quando esta configuração está desabilitada, o áudio é enviado e recebido via TCP.

Por padrão, o áudio sobre UDP é permitido.

### Plug N Play de áudio

Esta configuração permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som.

Por padrão, o uso de vários dispositivos de áudio é permitido.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

### Qualidade do áudio

Esta configuração especifica o nível de qualidade do som recebido nas sessões do usuário.

Por padrão, a qualidade do som é definida como Alta - áudio de alta definição.

Para controlar a qualidade do som, escolha uma das seguintes opções:

- Selecione Baixa - para conexões de baixa velocidade para conexões de baixa largura de banda. Os sons enviados para o dispositivo do usuário são compactados em até 16 Kbps. Essa compactação resulta em uma redução significativa na qualidade do som. Mas também permite um desempenho razoável para uma conexão de baixa largura de banda.
- Selecione Médio - otimizado para fala para fornecer aplicativos de Voz sobre Protocolo de Internet. Essa configuração entrega aplicativos de mídia em conexões de rede desafiadoras com linhas inferiores a 512 Kbps, ou congestionamento significativo e perda de pacotes. Este codec oferece tempo de codificação rápido, tornando-o ideal para uso com softphones e

aplicativos de Comunicações Unificadas quando você precisa de processamento de mídia no lado do servidor.

O áudio enviado para o dispositivo do usuário é compactado em até 64 Kbps. Essa compactação resulta em uma redução moderada na qualidade do áudio reproduzido no dispositivo do usuário, ao mesmo tempo em que oferece baixa latência e consome pouca largura de banda. Se a qualidade da Voz sobre Protocolo de Internet for insatisfatória, certifique-se de que a configuração da política de Transporte em Tempo Real de Áudio sobre UDP esteja definida como Permitido.

Agora, o Transporte em Tempo Real (RTP) sobre UDP é suportado apenas quando esta qualidade de áudio é selecionada. Use esta qualidade de áudio mesmo para entregar aplicativos de mídia para conexões de rede desafiadoras, como linhas de baixa velocidade (menos de 512 Kbps). Além disso, quando há congestionamento e perda de pacotes na rede.

- Selecione Alta - áudio de alta definição para conexões onde a largura de banda é abundante e a qualidade do som é importante. Os clientes podem reproduzir o som em sua taxa nativa. Os sons são compactados em um nível de alta qualidade, mantendo até a qualidade de CD e usando até 112 Kbps de largura de banda. A transmissão dessa quantidade de dados pode resultar em aumento do uso da CPU e congestionamento da rede.

A largura de banda é consumida apenas enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo de largura de banda dobra.

Para especificar a quantidade máxima de largura de banda, configure as configurações de **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem de limite de largura de banda de redirecionamento de áudio**.

**Redirecionamento de áudio do cliente**

Essa configuração especifica se os aplicativos hospedados no servidor podem reproduzir sons através de um dispositivo de som instalado no dispositivo do usuário. Essa configuração também especifica se os usuários podem gravar entrada de áudio.

Por padrão, o redirecionamento de áudio é permitido.

Após permitir esta configuração, você pode limitar a largura de banda consumida pela reprodução ou gravação de áudio. Limitar o consumo de largura de banda pelo áudio pode melhorar o desempenho do aplicativo, mas também pode degradar a qualidade do áudio. O consumo de banda ocorre apenas enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo de banda dobra. Para especificar a quantidade máxima de largura

de banda, configure as definições de **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem de limite de largura de banda de redirecionamento de áudio**.

Em máquinas com SO Windows Multi-session, certifique-se de que a configuração **Audio Plug N Play** esteja habilitada para suportar vários dispositivos de áudio.

Importante: Proibir o redirecionamento de áudio do cliente desabilita toda a funcionalidade de áudio HDX™.

#### Redirecionamento de microfone do cliente

Essa configuração habilita ou desabilita o redirecionamento do microfone do cliente. Quando habilitado, os usuários podem usar microfones para gravar entrada de áudio em uma sessão.

Por padrão, o redirecionamento de microfone é permitido.

Por segurança, os usuários são alertados quando servidores não confiáveis, por meio de seus dispositivos, tentam acessar microfones. Os usuários podem optar por aceitar ou não o acesso. Os usuários podem desabilitar o alerta no aplicativo Citrix Workspace™.

Em máquinas com SO Windows Multi-session, certifique-se de que a configuração Audio Plug N Play esteja Habilitada para suportar vários dispositivos de áudio.

Se a configuração de **Redirecionamento de áudio do cliente** estiver desabilitada no dispositivo do usuário, esta regra não terá efeito.

### Configurações de política de largura de banda

A seção **Largura de banda** inclui configurações de política para evitar problemas de desempenho relacionados ao uso da largura de banda da sessão do cliente.

Importante: O uso dessas configurações de política com as configurações da **política de Multi-Stream** pode produzir resultados inesperados. Se você usar as configurações de Multi-Stream em uma política, certifique-se de que essas configurações de política de limite de largura de banda não estejam incluídas.

#### Limite de largura de banda de redirecionamento de áudio

Esta configuração especifica a largura de banda máxima permitida para reproduzir ou gravar áudio em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de áudio

Esta configuração especifica o limite máximo de largura de banda permitido para reproduzir ou gravar áudio como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta configuração, também deverá configurar a configuração **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para as sessões do cliente.

### Limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB de e para o cliente. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de dispositivo USB do cliente**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB de e para o cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Client USB device redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite de largura de banda de redirecionamento da área de transferência

Esta configuração especifica a largura de banda máxima permitida para a transferência de dados entre uma sessão e a área de transferência local. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Clipboard redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento da área de transferência

Esta configuração especifica a largura de banda máxima permitida para a transferência de dados entre uma sessão e a área de transferência local como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Clipboard redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite de largura de banda de redirecionamento de porta COM

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica a largura de banda máxima permitida em kilobits por segundo para acessar uma porta COM em uma conexão de cliente. Se você inserir um valor para esta configuração e um valor para a configuração **COM port redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de porta COM

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as definições de redirecionamento de porta COM e porta LPT usando o registro.

Esta definição especifica a largura de banda máxima permitida para acessar portas COM em uma conexão de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado

Se você inserir um valor para esta definição e um valor para a definição **Limite de largura de banda de redirecionamento de porta COM**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se você configurar esta definição, você também deve configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente

**Limite de largura de banda da aceleração multimídia HDX™ MediaStream**

Esta definição especifica a largura de banda máxima permitida para acessar uma unidade de cliente em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta definição e um valor para a definição **Porcentagem do limite de largura de banda de redirecionamento de arquivo**, a definição mais restritiva (o valor mais baixo) entra em vigor.

**Porcentagem de limite de largura de banda de redirecionamento de arquivo**

Esta definição especifica o limite máximo de largura de banda permitido para acessar unidades de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta definição e um valor para a definição **Limite de largura de banda de redirecionamento de arquivo**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se você configurar esta definição, você também deve configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite de largura de banda de aceleração multimídia HDX™ MediaStream

Esta definição especifica o limite máximo de largura de banda permitido para entregar áudio e vídeo em streaming usando a Aceleração Multimídia HDX MediaStream. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) terá efeito.

### Limite de largura de banda percentual da aceleração multimídia HDX MediaStream

Esta configuração especifica a largura de banda máxima permitida para a entrega de áudio e vídeo em streaming usando a aceleração multimídia HDX MediaStream como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit**, a configuração mais restritiva (o valor mais baixo) terá efeito.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite de largura de banda de redirecionamento de porta LPT

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as definições de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica a largura de banda máxima permitida para trabalhos de impressão usando uma porta LPT em uma única sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **LPT port redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de porta LPT

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as definições de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica o limite de largura de banda para trabalhos de impressão usando uma porta LPT em uma única sessão de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **LPT port redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite geral de largura de banda da sessão

Esta configuração especifica a quantidade total de largura de banda disponível, em kilobits por segundo, para sessões de usuário.

O limite máximo de largura de banda aplicável é de 20 Mbps (20.000 Kbps). Por padrão, nenhum máximo (zero) é especificado.

Limitar a quantidade de largura de banda consumida por uma conexão de cliente pode melhorar o desempenho quando outros aplicativos fora da conexão de cliente estão competindo por largura de banda limitada.

### Limite de largura de banda de redirecionamento de impressora

Esta configuração especifica a largura de banda máxima permitida para acessar impressoras de cliente em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Printer redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de impressora

Esta configuração especifica a largura de banda máxima permitida para acessar impressoras de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Printer redirection bandwidth limit**, a configuração mais restritiva (com o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

### Limite de largura de banda de redirecionamento de dispositivo TWAIN

Esta configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN a partir de aplicativos publicados. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN**, a configuração mais restritiva (o valor mais baixo) será aplicada.

### Porcentagem de limite de largura de banda de redirecionamento de dispositivo TWAIN

Esta configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN de aplicativos publicados como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de dispositivo TWAIN**, a configuração mais restritiva (com o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

## Configurações de política de redirecionamento de conteúdo bidirecional

A seção **Redirecionamento de Conteúdo Bidirecional** possui configurações de política para habilitar ou desabilitar o redirecionamento de URL cliente-para-VDA e VDA-para-cliente.

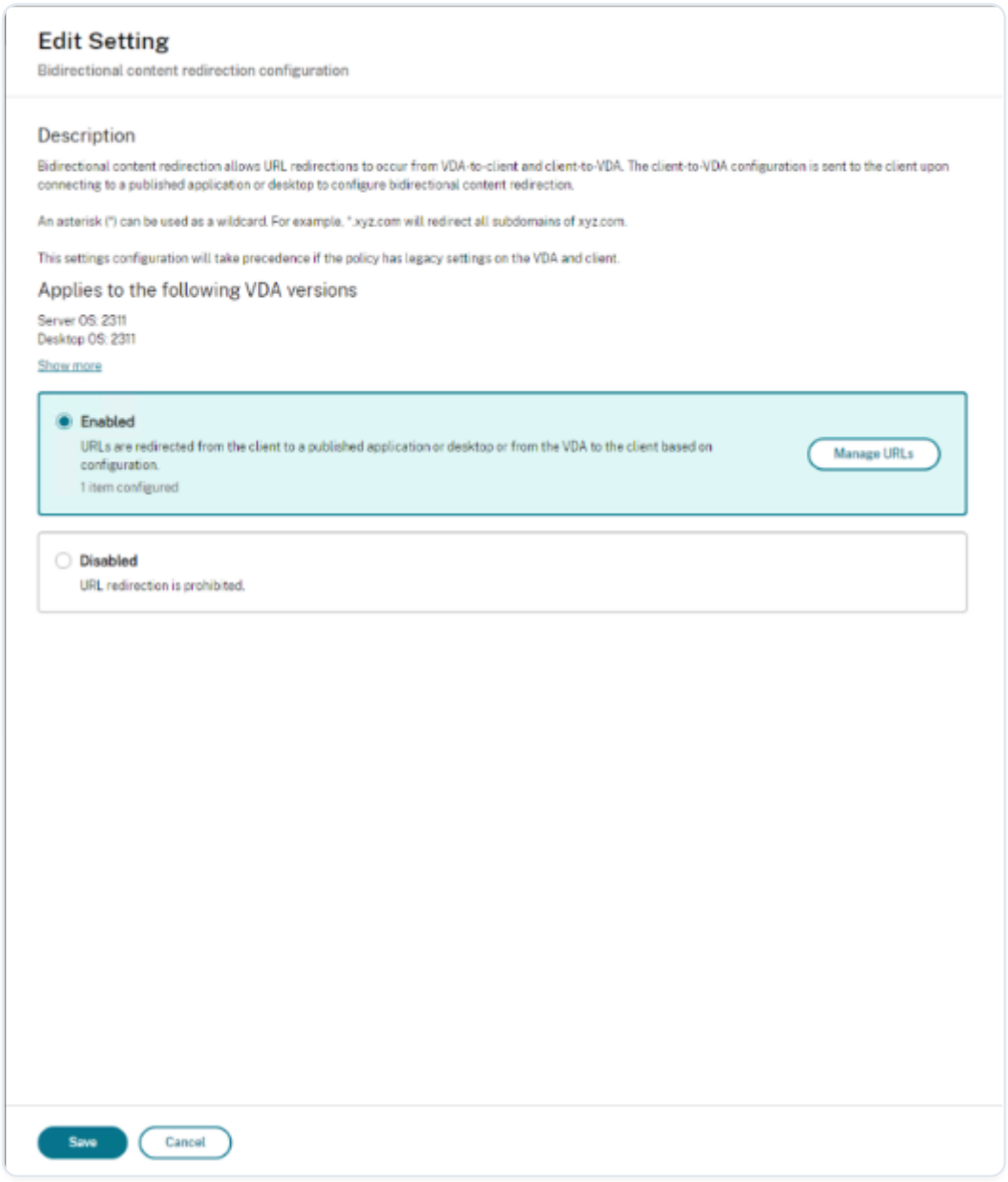
As políticas de servidor são definidas no Web Studio. A partir da versão 2311 do aplicativo Citrix Workspace™, essa configuração substitui as três configurações legadas a seguir no Web Studio que foram descontinuadas:

- Permitir redirecionamento de conteúdo bidirecional
- URLs permitidas para serem redirecionadas para VDA
- URLs permitidas para serem redirecionadas para o Cliente

Ela também substitui as três configurações de Objeto de Política de Grupo (GPO) locais a seguir em clientes Windows:

- Redirecionamento de conteúdo bidirecional
- Substituições de redirecionamento de conteúdo bidirecional
- Redirecionamento OAuth

Se essa configuração estiver habilitada, as configurações cliente-para-VDA são enviadas ao cliente ao se conectar a um aplicativo ou desktop publicado para configurar o redirecionamento de conteúdo bidirecional.




Se essa configuração for configurada, ela terá precedência sobre as configurações legadas no Web Studio e no cliente. A Citrix® recomenda usar apenas as novas configurações de política e excluir quaisquer configurações legadas para evitar comportamentos inesperados.

As políticas de cliente não devem ser definidas se o VDA e o DDC estiverem executando a versão 2311 ou posterior. Caso contrário, as políticas de cliente são definidas a partir do modelo administrativo de Objeto de Política de Grupo do aplicativo Citrix Workspace.

A Citrix oferece redirecionamento host-para-cliente e Acesso a Aplicativos Locais para redirecionamento cliente-para-URL. No entanto, a Citrix recomenda que você use o redirecionamento de conteúdo bidirecional para clientes Windows ingressados no domínio.

A Citrix recomenda usar a nova interface de usuário no Web Studio para configurar o recurso em vez do Desktop Studio.

### Redirecionamento curinga

O redirecionamento de conteúdo bidirecional suporta o uso de curingas ao definir as URLs a serem redirecionadas. Para obter mais detalhes e configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de Configuração. No Web Studio, defina a URL curinga editando a string JSON como um valor na chave `url` no array `hostToClientUrls` ou no array `clientToHostUrls`.

> **Observação:**
>
> - Não defina a mesma URL em `hostToClientUrls` e `clientToHostUrls` para evitar loops infinitos.
> - Domínios de nível superior não são suportados. Por exemplo, `<https://www.citrix.*>` ou `<http://www.citrix.co*>` não é redirecionado.

### Configuração de redirecionamento de conteúdo bidirecional

Defina esta política como `Enabled` para começar a configurar o recurso e clique em **Gerenciar URLs**. Defina as seguintes configurações:

- **Redirecionamento de VDA para cliente**
- **Redirecionamento de cliente para VDA**

#### REDIRECIONAMENTO DE VDA PARA CLIENTE

Para redirecionar URLs do VDA para o cliente, insira uma URL por linha. Curingas são permitidos. O redirecionamento OAuth permite que você use o navegador no endpoint do cliente para realizar a autenticação e enviar o token de volta para o VDA.

**Benefícios:**

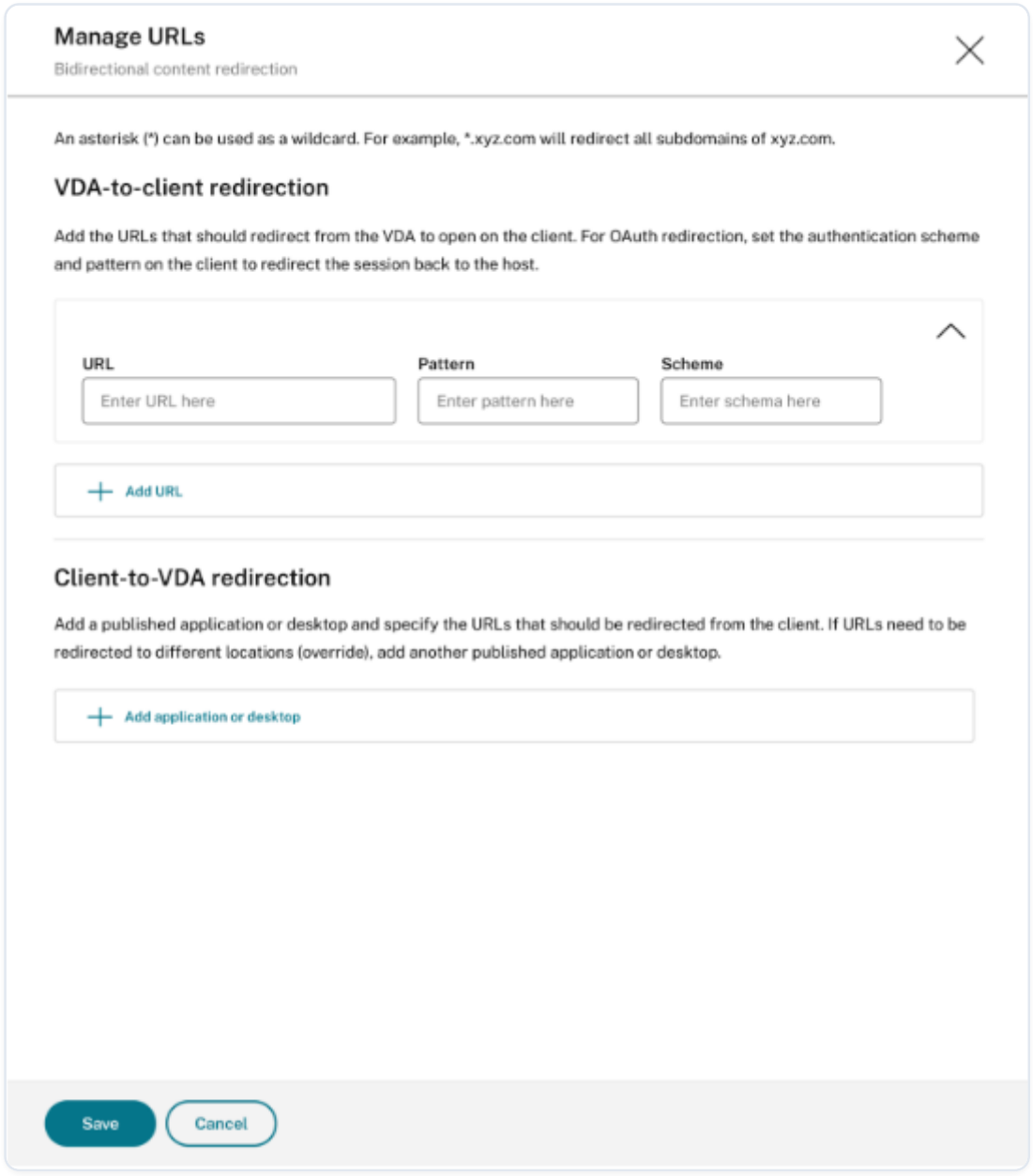
- Você pode evitar armazenar essas credenciais no ambiente hospedado.
- Você pode usar recursos biométricos que estão disponíveis no endpoint e não no VDA.

**Configurações:**

Para configurar o redirecionamento de VDA para cliente para a URL, especifique o seguinte:

- **URL** (Obrigatório) Adicione a URL que deve ser redirecionada do VDA para abrir no cliente. Para **Redirecionamento OAuth**, defina o esquema de autenticação e o padrão no cliente para redirecionar a sessão de volta ao host.

- **Padrão**: (Opcional) Expressão regular de URL que, quando redirecionada para o cliente através do redirecionamento de URL de VDA para Cliente, é rastreada como se um fluxo de autenticação OAuth tivesse começado, e quando o fluxo é concluído (detectado pelo esquema resultante ou padrão de URL de redirecionamento sendo aberto), essa URL resultante é redirecionada de volta para o VDA host que iniciou esse fluxo.
- **Esquema**: (Opcional) Se o **Esquema** for especificado, a URL de término deverá ter o formato: `<scheme>`:// `<something>`. Considere que o Esquema não foi especificado (vazio). Nesse caso, o padrão de URL resultante original é extraído do Padrão através de um grupo de captura de expressão regular (deve ser especificado no Padrão), e a URL original é reescrita para usar uma URL de redirecionamento `citrix-oauth-redir://`. Quando o fluxo é concluído, a URL de redirecionamento original é então redirecionada de volta para o Host (VDA). Neste caso, qualquer servidor de Autorização OAuth deve ser configurado para permitir URLs de redirecionamento `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.




**Observação:**

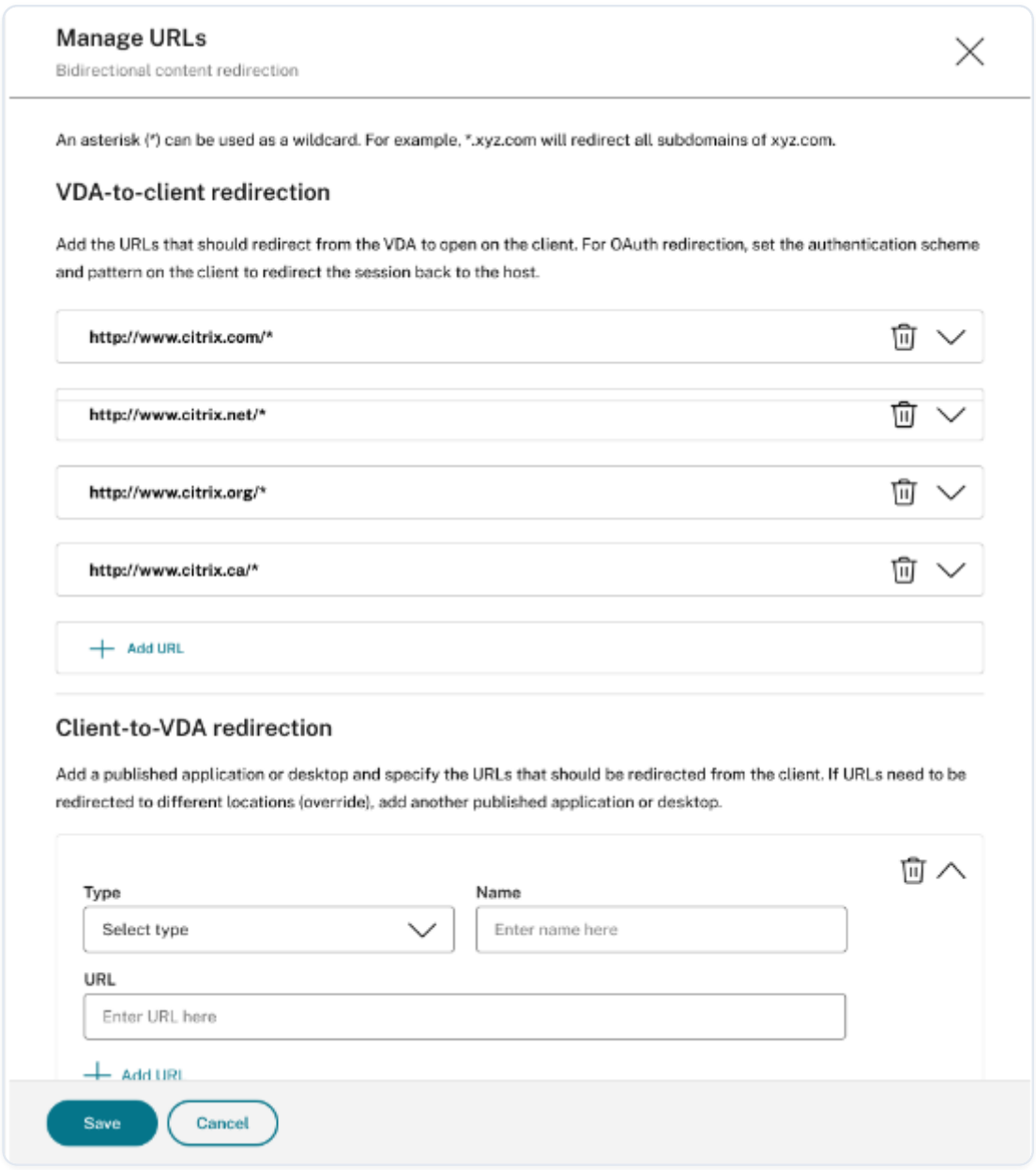
Embora tanto o **Padrão** quanto o **Esquema** sejam opcionais, se o **Padrão** for especificado, você também deve especificar o **Esquema**.

### REDIRECIONAMENTO DO CLIENTE PARA O VDA

Para redirecionar URLs do cliente para o VDA, conclua as seguintes etapas:

1. Configure o destino para as URLs do cliente.
2. Selecione Aplicativo Publicado ou Área de Trabalho Publicada.
3. Especifique o nome desse recurso.

4. Adicione todas as URLs que devem ser redirecionadas para esse recurso. Você pode substituir esse recurso padrão adicionando um novo aplicativo ou área de trabalho e, em seguida, especificando as URLs a serem redirecionadas para esse recurso.




## DESKTOP STUDIO

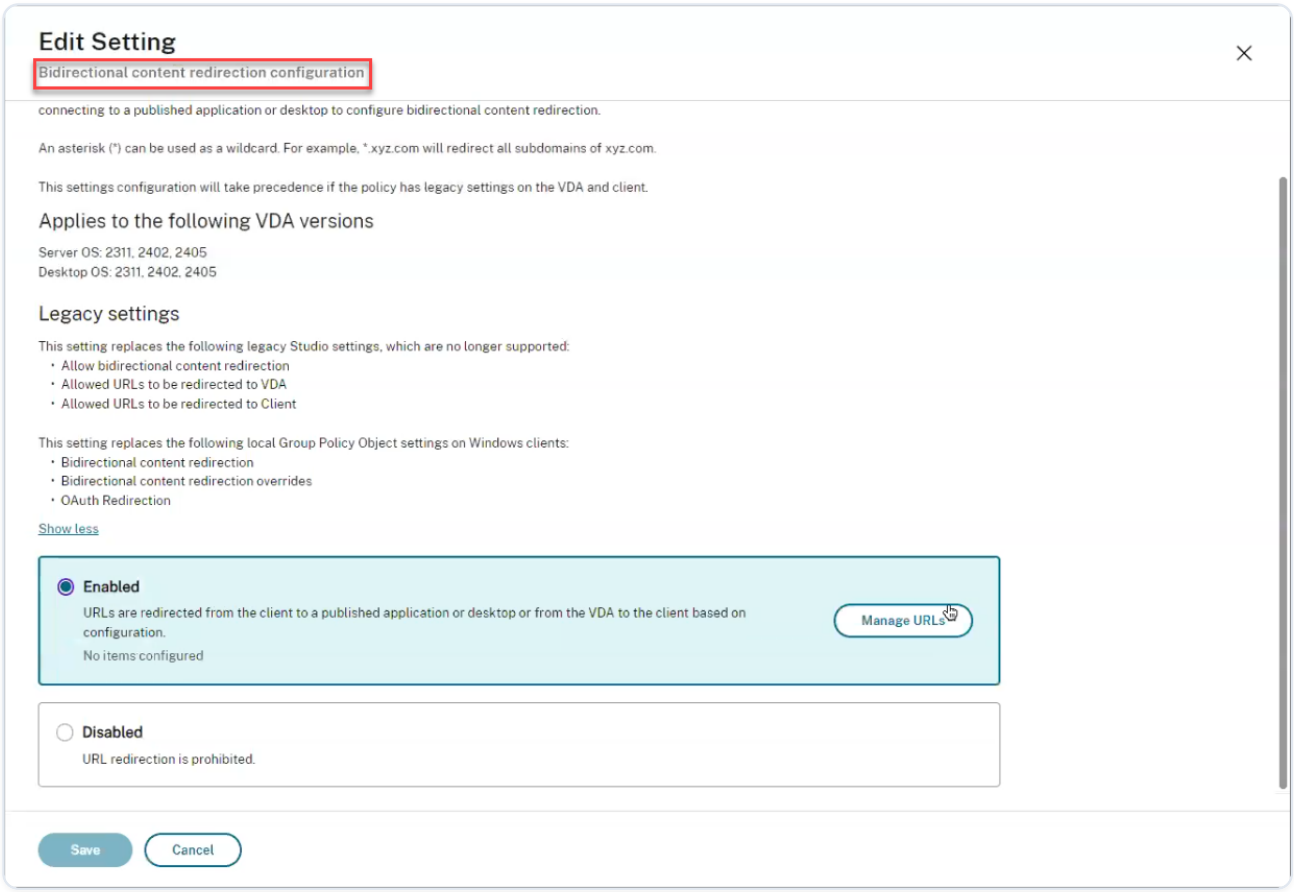
**Observação:**

A Citrix recomenda usar o Web Studio para configurar esse recurso a partir da versão 2402 do Citrix Virtual Apps and Desktops™.

Para configurar o redirecionamento de conteúdo bidirecional para 2311, crie uma string JSON com o seguinte formato:

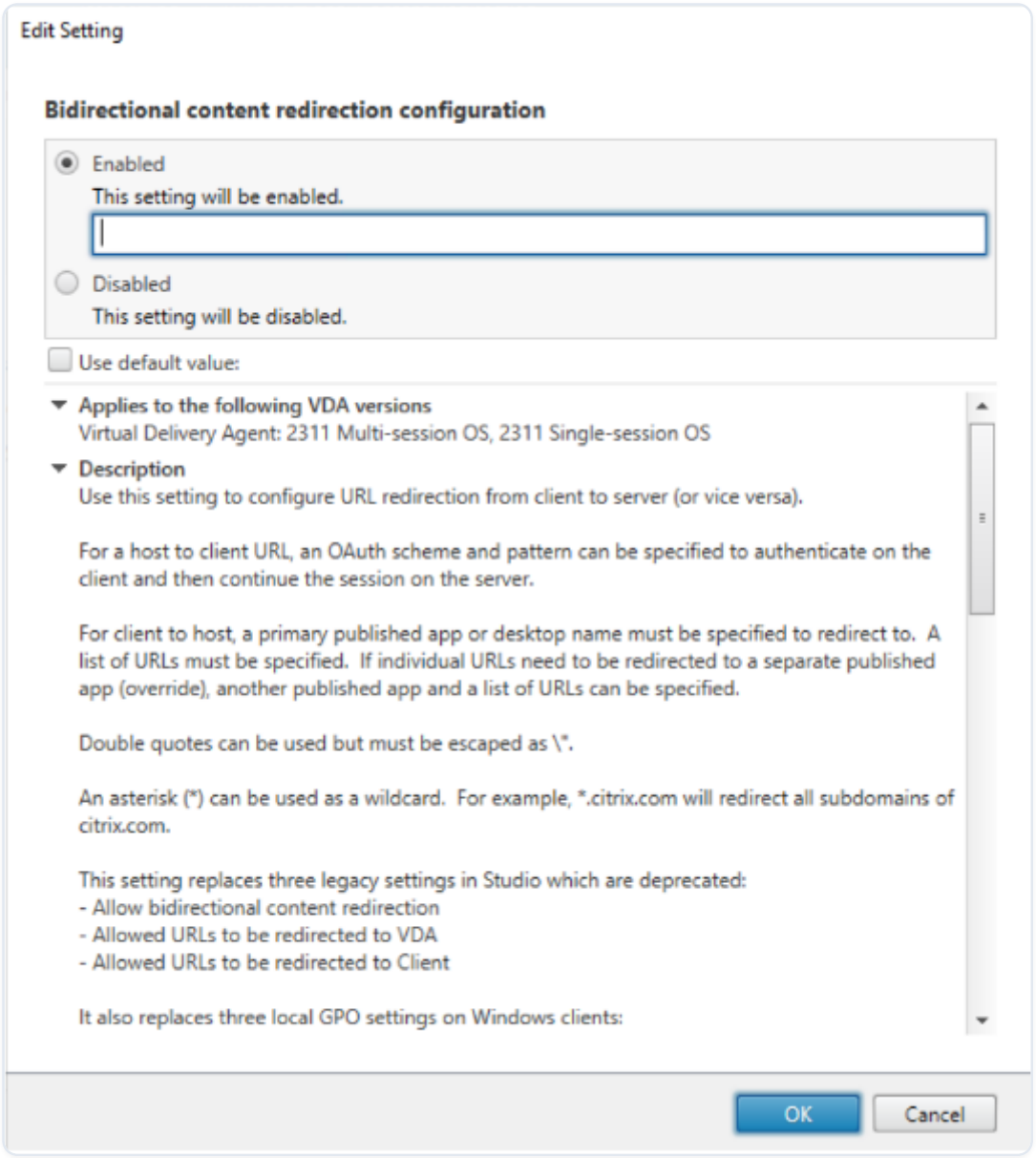
```
{
  "version": 1,
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```




Os seguintes parâmetros devem ser definidos:

- **version**: (Obrigatório) Defina como 1.
- Para redirecionamento de URL do VDA para o cliente, crie um único `hostToClientConfig`.
- `hostToClientUrls`: (Obrigatório) Lista de URLs a serem redirecionadas do host (VDA) para o cliente. Curingas são permitidos. Se `hostToClientConfig` for especificado, mas o redirecionamento do cliente para o host VDA não for necessário, então `clientToHostConfig` deve ser especificado com `publishedAppOrDesktopNameType`, um `publishedAppOrDesktopName` vazio e um `clientToHostUrls` vazio.




### Redirecionamento OAuth

O redirecionamento OAuth permite que você use o navegador do endpoint do cliente para autenticar e envie o token de volta para o VDA.

**Benefícios**:

- Você pode evitar armazenar essas credenciais no ambiente hospedado.
- Você pode usar recursos biométricos que estão disponíveis no endpoint e não no VDA.

Para configurar o redirecionamento OAuth para a URL, especifique os seguintes parâmetros:

- **oAuthRedirectionPattern**: (Opcional) Expressão regular de URL que, quando redirecionada para o cliente via redirecionamento de URL VDA-para-Cliente, é rastreada como se um fluxo de autenticação OAuth tivesse começado, e quando o fluxo é concluído (detectado pelo

esquema resultante ou padrão de URL de redirecionamento sendo aberto), essa URL resultante é redirecionada de volta para o VDA host que iniciou esse fluxo.

- **oAuthScheme**: (Opcional) Se um Esquema for especificado, espera-se que a URL de término esteja no formato: `<scheme>`:// `<something>`. Considere que o Esquema não foi especificado (vazio). Nesse caso, o padrão de URL resultante original é extraído do Padrão por meio de um grupo de captura de expressão regular (deve ser especificado no Padrão), e a URL original é reescrita para usar uma URL de redirecionamento `citrix-oauth-redir://`. Quando o fluxo é concluído, a URL de redirecionamento original é então redirecionada de volta para o Host (VDA). Neste caso, qualquer servidor de Autorização OAuth deve ser configurado para permitir URLs de redirecionamento `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.

Para um redirecionamento cliente-para-VDA, crie **clientToHostConfig** para cada recurso a ser redirecionado. Para cada recurso, inclua os seguintes parâmetros:

- **publishedAppOrDesktopNameType**: (Obrigatório) Um desktop publicado (“Desktop”) ou um aplicativo publicado (“Application”) configurado no Web Studio. Se o recurso não for válido, o redirecionamento não funcionará corretamente.
- **publishedAppOrDesktopName**: (Obrigatório) Nome do recurso conforme configurado no Web Studio.
- **clientToHostUrls**: (Obrigatório) Lista de URLs a serem redirecionadas do cliente para o host (VDA). curingas são permitidos.

#### Limitação conhecida

Ao iniciar um navegador usando o PowerShell com um esquema de URL personalizado (não HTTP ou HTTPS), as URLs personalizadas não são redirecionadas para o cliente.

### Configurações de política de redirecionamento de conteúdo do navegador

A seção de redirecionamento de conteúdo do navegador inclui configurações de política para configurar esse recurso.

O redirecionamento de conteúdo do navegador controla e otimiza a forma como o Citrix Virtual Apps and Desktops™ entrega qualquer conteúdo de navegador da web (por exemplo, HTML5) aos usuários. Apenas a área visível do navegador onde o conteúdo é exibido é redirecionada.

O redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador são recursos independentes. As políticas de redirecionamento de vídeo HTML5 não são necessárias para que esse recurso funcione. No entanto, o Citrix HDX HTML5 Video Redirection Service é

usado para o redirecionamento de conteúdo do navegador. Para obter mais informações, consulte Redirecionamento de conteúdo do navegador.

> **Observação:**
>
> As configurações de política disponíveis no Web Studio podem ser substituídas por chaves de registro no VDA, mas as chaves de registro são opcionais.

### TLS e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) em execução no VDA. Para conseguir esse redirecionamento e manter a integridade TLS da página da web, o Citrix HDX HTML5 Video Redirection Service gera dois certificados personalizados no armazenamento de certificados no VDA.

HdxVideo.js usa Secure Web sockets para se comunicar com o WebSocketService.exe em execução no VDA. Este processo é executado no Sistema Local e realiza a terminação SSL e o mapeamento de sessão do usuário.

O WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

### Redirecionamento de conteúdo do navegador

Por padrão, o aplicativo Citrix Workspace™ tenta a busca e renderização do cliente. A renderização do lado do servidor é tentada quando a busca e renderização do cliente falham. Se você também habilitar a política de configuração de proxy de redirecionamento de conteúdo do navegador, o aplicativo Citrix Workspace tentará apenas a busca do servidor e a renderização do cliente.

Por padrão, essa configuração é Permitida.

### Configuração de suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

O redirecionamento de conteúdo do navegador habilita a sobreposição que usa o esquema Negotiate para autenticação. Esse aprimoramento fornece logon único a um servidor web configurado com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio do VDA.

Quando definido como **Permitido**, a sobreposição de redirecionamento de conteúdo do navegador obtém um tíquete Negotiate usando as credenciais do VDA do usuário. O usuário então se autentica no servidor web com um logon único.

Quando definido como **Proibido**, a sobreposição de redirecionamento de conteúdo do navegador não solicita um tíquete Negotiate do VDA. O usuário se autentica em um servidor web usando um método de autenticação básico. Este método de autenticação exige que os usuários insiram suas credenciais VDA cada vez que acessam o servidor web.

Por padrão, esta configuração é Proibida.

### Configuração de autenticação de proxy web de busca de servidor de redirecionamento de conteúdo do navegador

Esta configuração roteia o tráfego HTTP originado em uma sobreposição através de um proxy web downstream. O proxy web downstream autoriza e autentica o tráfego HTTP usando as credenciais de domínio do usuário VDA através do esquema de autenticação Negotiate.

Você deve configurar o redirecionamento de conteúdo do navegador para o modo de busca de servidor no arquivo PAC usando a política de configuração de proxy de redirecionamento de conteúdo do navegador. No script PAC, forneça instruções para rotear o tráfego da sobreposição através de um proxy web downstream. Em seguida, configure o proxy web downstream para autenticar os usuários VDA através do esquema de autenticação Negotiate.

Quando definido como **Permitido**, o proxy web responde com um desafio 407 Negotiate, incluindo um cabeçalho **Proxy-autenticar: Negotiate**. O redirecionamento de conteúdo do navegador então obtém um tíquete de serviço Kerberos usando as credenciais de domínio do usuário VDA. Além disso, inclua o tíquete de serviço em solicitações posteriores ao proxy web.

Quando definido como **Proibido**, o redirecionamento de conteúdo do navegador faz proxy de todo o tráfego TCP entre a sobreposição e o proxy web sem interferir. A sobreposição usa credenciais de autenticação básicas ou quaisquer outras credenciais disponíveis para autenticar no proxy web.

Por padrão, esta configuração é Proibida.

### Configurações da política de configuração de ACL (Lista de Controle de Acesso) de redirecionamento de conteúdo do navegador

Use esta configuração para configurar uma Lista de Controle de Acesso (ACL) de URLs que podem usar o redirecionamento de conteúdo do navegador ou que têm o acesso negado ao redirecionamento de conteúdo do navegador.

URLs autorizadas são as URLs na lista de permissões cujo conteúdo é redirecionado para o cliente.

O curinga `*` é permitido, mas não é permitido dentro do protocolo ou da parte do endereço de domínio da URL. No entanto, a partir do Citrix Virtual Apps and Desktops 7 2206, o curinga `*` é permitido dentro da parte do endereço de subdomínio da URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Não permitido: `http://*.*.com/`

Você pode obter uma granularidade melhor especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, apenas a página index.html será redirecionada.

Por padrão, esta configuração é definida como `https://www.youtube.com/*`

Para mais informações, consulte o artigo da Central de Conhecimento CTX238236.

> **Observação:**
>
> Você pode configurar a ACL para permitir que o BCR redirecione sites para o endpoint e os sites de autenticação podem ser configurados para permitir Provedores de Identidade (IdP), como Okta e Duo, para autenticação usada na URL configurada.

**Sites de autenticação de redirecionamento de conteúdo do navegador**

Use esta configuração para configurar uma lista de URLs. Os sites redirecionados usando o redirecionamento de conteúdo do navegador usam a lista para autenticar um usuário. A configuração especifica as URLs para as quais o redirecionamento de conteúdo do navegador permanece ativo (redirecionado) ao navegar para fora de uma URL na lista de permissões.

Um cenário clássico é um site que depende de um Provedor de Identidade (IdP) para autenticação. Por exemplo, um site `www.xyz.com` deve ser redirecionado para o endpoint, mas um IdP de terceiros, como Okta (`www.xyz.okta.com`), lida com a parte da autenticação. O administrador usa a política de configuração de ACL de redirecionamento de conteúdo do navegador para adicionar `www.xyz.com` à lista de permissões. Em seguida, usa os sites de autenticação de redirecionamento de conteúdo do navegador para adicionar `www.xyz.okta.com` à lista de permissões.

Para mais informações, consulte o artigo da Central de Conhecimento CTX238236.

### Configuração da lista de bloqueio de redirecionamento de conteúdo do navegador

Esta configuração funciona em conjunto com a configuração de ACL de redirecionamento de conteúdo do navegador. Considere que as URLs estão presentes na configuração de ACL de redirecionamento de conteúdo do navegador e na configuração da lista de bloqueio. Neste caso, a configuração da lista de bloqueio tem precedência e o conteúdo do navegador da URL não é redirecionado.

**URLs não autorizadas:** Especifica as URLs na lista de bloqueio cujo conteúdo do navegador não é redirecionado para o cliente, mas renderizado no servidor.

O curinga * é permitido, mas não é permitido dentro do protocolo ou da parte do endereço de domínio da URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Não permitido: `http://*.xyz.com/`

Você pode obter maior granularidade especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, apenas index.html estará na lista de bloqueio.

### Configuração de proxy de redirecionamento de conteúdo do navegador

Esta configuração fornece opções de configuração para as configurações de proxy no VDA para redirecionamento de conteúdo do navegador. Se ativado com um endereço de proxy e número de porta válidos, URL PAC / WPAD ou configuração Direta/Transparente, o aplicativo Citrix Workspace tenta apenas a busca no servidor e a renderização no cliente.

Se desativado ou não configurado e usando um valor padrão, o aplicativo Citrix Workspace tenta a busca no cliente e a renderização no cliente.

Por padrão, esta configuração é Proibida.

**Padrão permitido para um proxy explícito:**

`http://<hostname/ip address\>:\<port\>`

**Exemplo:**

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

**Padrões permitidos para arquivos PAC/WPAD:**

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

**Exemplo:** `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

**Exemplo:** `http://10.10.10.10/configuration/pac/wpad.dat`

**Padrões permitidos para proxies diretos ou transparentes:**

Digite a palavra **DIRECT** na caixa de texto da política.

**Substituições de chave de registro de redirecionamento de conteúdo do navegador**

> **Aviso:**

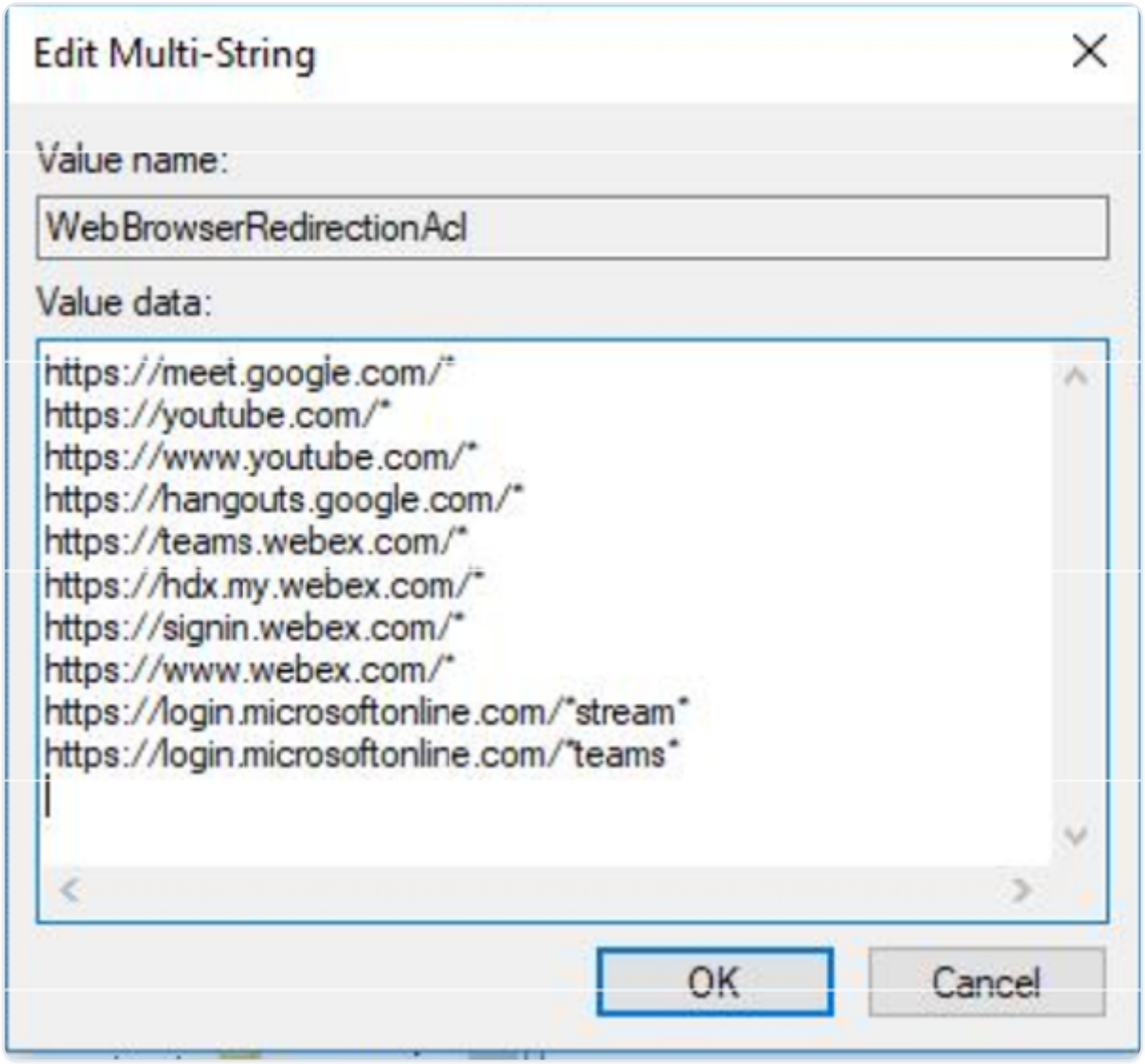
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se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

> Opções de substituição do registro para configurações de política:

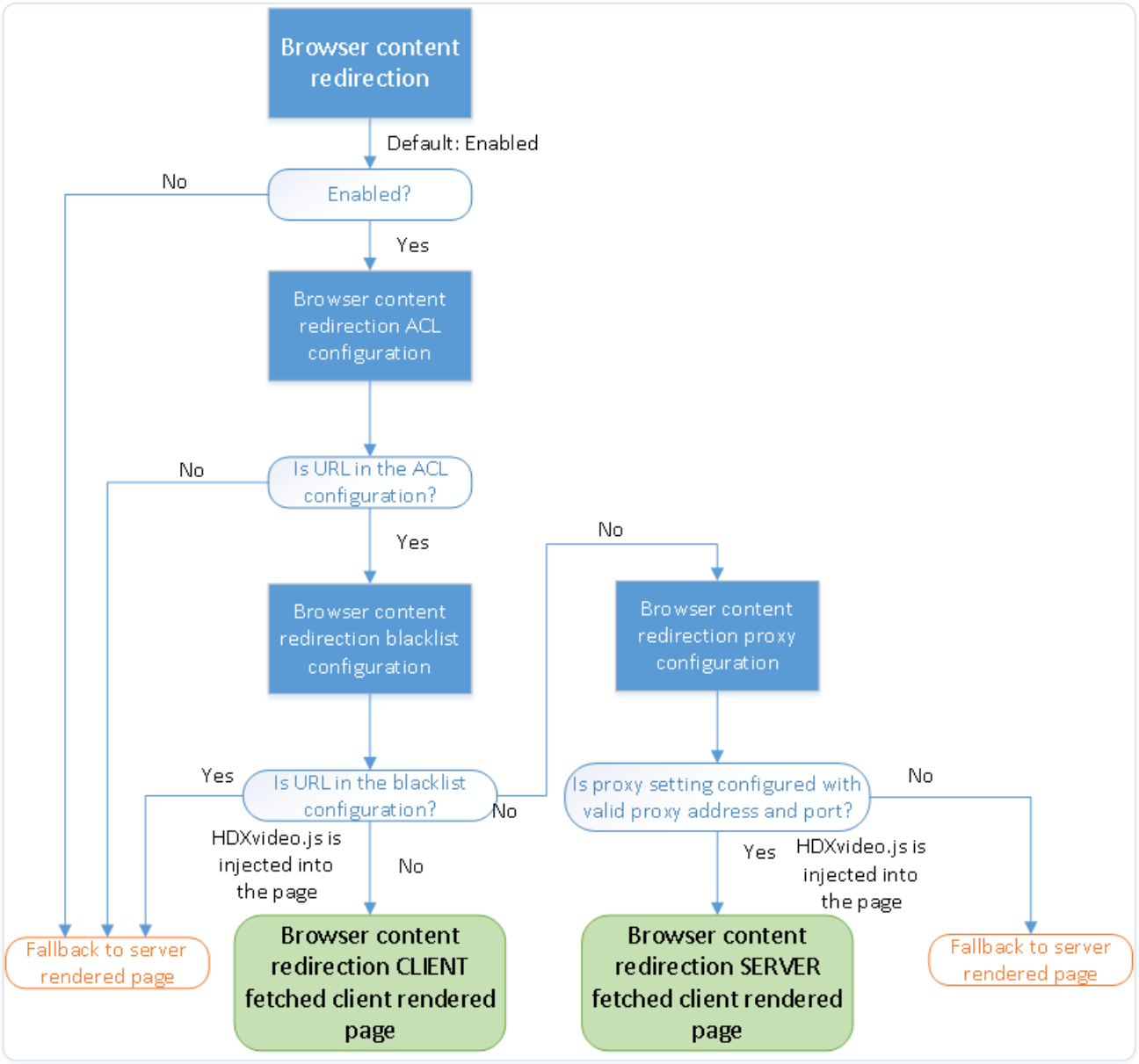
`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

| NOME | TIPO | VALOR |
|---|---|---|
| WebBrowserRedirection | DWORD | 1=Permitido, 0=Proibido |
| WebBrowserRedirectionAcl | REG_MULTI_SZ | |
| WebBrowserRedirectionAuthenticationSites | REG_MULTI_SZ | |
| WebBrowserRedirectionProxyAddress | REG_SZ | `http://myproxy.citrix.com:8080` ou `http://10.10.10.10:8888` |

| NOME | TIPO | VALOR |
| --- | --- | --- |
| WebBrowserRedirectionBlacklist | REG_MULTI_SZ | |



### Inserção de HDXVideo.js para redirecionamento de conteúdo do navegador




O HdxVideo.js é injetado na página da web usando a extensão do Chrome de redirecionamento de conteúdo do navegador ou o Objeto Auxiliar do Navegador (BHO) do Internet Explorer. O BHO é um modelo de plug-in para o Internet Explorer. Ele fornece ganchos para APIs do navegador e permite que o plug-in acesse o Modelo de Objeto de Documento (DOM) da página para controlar a navegação.

O BHO decide se injeta o HdxVideo.js em uma determinada página. A decisão é baseada nas políticas administrativas mostradas no fluxograma anterior.

Depois que ele decide injetar o JavaScript e redirecionar o conteúdo do navegador para o cliente, a página da web fica em branco no navegador Internet Explorer no VDA. Definir o **document.body.innerHTML** como vazio remove todo o corpo da página da web no VDA. A página está pronta para ser enviada ao cliente para ser exibida no navegador de sobreposição (Hdxbrowser.exe) no cliente.

## Configurações de política de sensores do cliente

A seção **Sensores do Cliente** inclui configurações de política para controlar como as informações do sensor do dispositivo móvel são tratadas em uma sessão de usuário.

### Permitir que aplicativos usem a localização física do dispositivo cliente

Esta configuração determina se os aplicativos em execução em uma sessão em um dispositivo móvel têm permissão para usar a localização física do dispositivo do usuário.

Por padrão, o uso de informações de localização é proibido

Quando esta configuração é proibida, as tentativas de um aplicativo de recuperar informações de localização retornam um valor de "permissão negada".

Quando esta configuração é permitida, um usuário pode proibir o uso de informações de localização negando uma solicitação do aplicativo Citrix Workspace™ para acessar a localização. Dispositivos Android e iOS solicitam na primeira vez que as informações de localização são requisitadas em cada sessão.

Ao desenvolver aplicativos hospedados que usam a configuração Permitir que aplicativos usem a localização física do dispositivo cliente, considere o seguinte:

- Certifique-se de que um aplicativo habilitado para localização não dependa da disponibilidade de informações de localização porque:
  - Um usuário pode não permitir o acesso às informações de localização.
  - A localização pode não estar disponível ou pode mudar enquanto o aplicativo está em execução.
  - Um usuário pode se conectar à sessão do aplicativo a partir de um dispositivo diferente que não suporte informações de localização.
- Um aplicativo habilitado para localização deve:
  - Ter o recurso de localização desativado por padrão.
  - Fornecer ao usuário uma opção para permitir ou não o recurso enquanto o aplicativo está em execução.
  - Ofereça ao usuário uma opção para limpar os dados de localização que o aplicativo armazena em cache. (O aplicativo Citrix Workspace não armazena dados de localização em cache.)

- Um aplicativo habilitado para localização deve gerenciar a granularidade das informações de localização. Essa gestão garante que os dados adquiridos sejam apropriados para a finalidade do aplicativo. Além disso, está em conformidade com os regulamentos em todas as jurisdições relevantes.
- Imponha uma conexão segura (por exemplo, usando TLS ou uma VPN) ao usar serviços de localização. Conecte o aplicativo Citrix Workspace a servidores confiáveis.
- Considere obter aconselhamento jurídico em relação ao uso de serviços de localização.

## Configurações de política da UI da área de trabalho

A seção **Interface do Usuário da Área de Trabalho** inclui configurações de política que controlam efeitos visuais como papel de parede da área de trabalho, animações de menu e imagens de arrastar. Essas configurações de política ajudam a gerenciar a largura de banda usada nas conexões de cliente. Você pode melhorar o desempenho do aplicativo em uma WAN limitando o uso da largura de banda.

**Importante:**

Não oferecemos suporte ao modo gráfico herdado e à Redireção de Composição da Área de Trabalho (DCR) nesta versão. Esta política é incluída apenas para compatibilidade com versões anteriores ao usar:

- XenApp 7.15 LTSR
- XenDesktop 7.15 LTSR
- Versões anteriores do VDA com Windows 7 e Windows 2008 R2.

### Redirecionamento de Composição da Área de Trabalho

Esta configuração especifica se devem ser usadas as capacidades de processamento do seguinte para renderização gráfica DirectX local, a fim de proporcionar aos usuários uma experiência de área de trabalho Windows mais fluida:

- Unidade de processamento gráfico (GPU) no dispositivo do usuário
- Ou,
- Processador gráfico integrado (IGP) no dispositivo do usuário

Quando ativado, o **Redirecionamento de Composição da Área de Trabalho** oferece uma experiência Windows altamente responsiva, mantendo alta escalabilidade no servidor.

Por padrão, o **Redirecionamento de Composição da Área de Trabalho** está desativado.

Para desmarcar **Redirecionamento de Composição da Área de Trabalho** e reduzir a largura de banda necessária nas sessões do usuário, selecione **Desativado** ao adicionar esta configuração a uma política.

### Qualidade gráfica da Redireção de Composição da Área de Trabalho

Esta configuração especifica a qualidade dos gráficos usados para a Redireção de Composição da Área de Trabalho.

O padrão é Alto.

Escolha entre qualidade Alta, Média, Baixa ou Sem Perdas.

### Papel de parede da área de trabalho

Essa configuração permite ou impede a exibição de papel de parede nas sessões do usuário.

Por padrão, as sessões do usuário podem exibir papel de parede.

Para desmarcar o papel de parede da área de trabalho e reduzir a largura de banda necessária nas sessões do usuário, selecione **Proibido** ao adicionar essa configuração a uma política.

### Animação de menu

Essa configuração permite ou impede a animação de menu nas sessões do usuário.

Por padrão, a animação de menu é permitida.

A animação de menu é uma configuração de preferência pessoal da Microsoft para facilitar o acesso. Quando ativada, ela faz com que um menu apareça após um pequeno atraso, seja rolando ou aparecendo gradualmente. Um ícone de seta aparece na parte inferior do menu. O menu aparece quando você aponta para essa seta.

A animação de menu é ativada em uma área de trabalho se essa configuração de política estiver definida como **Permitido** e a configuração de preferência pessoal da Microsoft para animação de menu estiver ativada.

> **Nota:**

> As alterações na configuração de preferência pessoal da Microsoft para animação de menu afetam a área de trabalho. Considere que você configurou a área de trabalho para descartar as alterações quando a sessão termina. Nesse caso, um usuário que ativou as animações de menu pode não ter animação de menu em sessões subsequentes. Para usuários que exigem animação de menu, ative a configuração da Microsoft na imagem principal da área de trabalho ou garanta que a área de trabalho retenha as alterações do usuário.

#### Visualizar conteúdo da janela ao arrastar

Essa configuração permite ou impede a exibição do conteúdo da janela ao arrastar uma janela pela tela.

Por padrão, a visualização do conteúdo da janela é permitida.

Quando definido como **Permitido**, a janela inteira parece se mover quando você a arrasta. Quando definido como **Proibido**, apenas o contorno da janela parece se mover até que você a solte.

### Configurações de política de monitoramento do usuário final

A seção **Monitoramento do Usuário Final** inclui configurações de política para medir o tráfego da sessão.

#### Cálculo de ida e volta do ICA®

Esta configuração determina se os cálculos de ida e volta do ICA são feitos para conexões ativas.

Por padrão, os cálculos para conexões ativas estão ativados.

Por padrão, cada início de medição de ida e volta do ICA é atrasado. Esse atraso ocorre até que algum tráfego que indique interação do usuário aconteça. Esse atraso pode ter duração indefinida e foi projetado para evitar que a medição de ida e volta do ICA seja a única razão para o tráfego do ICA.

#### Intervalo de cálculo de ida e volta do ICA

Esta configuração especifica a frequência, em segundos, com que os cálculos de ida e volta do ICA são realizados.

Por padrão, a ida e volta do ICA é calculada a cada 15 segundos.

#### Cálculos de ida e volta do ICA para conexões ociosas

Esta configuração determina se os cálculos de ida e volta do ICA são feitos para conexões ociosas.

Por padrão, os cálculos não são realizados para conexões ociosas.

Por padrão, cada início de medição de ida e volta do ICA é atrasado. Esse atraso ocorre até que algum tráfego que indique interação do usuário aconteça. Esse atraso pode ter duração indefinida e foi projetado para evitar que a medição de ida e volta do ICA seja a única razão para o tráfego do ICA.

### Configuração da política de experiência de área de trabalho aprimorada

A configuração da política de experiência de área de trabalho aprimorada executa sessões em sistemas operacionais de servidor que se parecem com áreas de trabalho locais do Windows 7.

Por padrão, esta configuração é permitida.

Se um perfil de usuário com o tema Clássico do Windows existir na área de trabalho virtual, esta política não fornecerá uma experiência de área de trabalho aprimorada para esse usuário. Considere um usuário com um perfil de usuário com tema do Windows 7 que faz logon em uma área de trabalho virtual executando o Windows Server 2012. Além disso, esta política não está configurada ou está desabilitada. Nesse caso, esse usuário vê uma mensagem de erro indicando falha ao aplicar o tema.

Em ambos os casos, redefinir o perfil do usuário resolve o problema.

Se você desabilitar a política em uma área de trabalho virtual com sessões de usuário ativas, a interface dessas sessões se tornará inconsistente em áreas de trabalho do Windows 7 e Windows Clássico. Para evitar essa inconsistência, certifique-se de reiniciar a área de trabalho virtual após alterar essa configuração de política. Em seguida, exclua quaisquer perfis de usuário móveis na área de trabalho virtual. A Citrix® também recomenda excluir quaisquer outros perfis de usuário na área de trabalho virtual para evitar inconsistências entre os perfis.

Considere que você está usando perfis de usuário móveis em seu ambiente. Nesse caso, certifique-se de que o recurso Experiência de Área de Trabalho Aprimorada esteja habilitado ou desabilitado para todas as áreas de trabalho virtuais que compartilham um perfil.

A Citrix não recomenda compartilhar perfis de usuário móveis entre áreas de trabalho virtuais que executam sistemas operacionais de servidor e sistemas operacionais de cliente. Os perfis para sistemas operacionais de cliente e servidor diferem. O compartilhamento de perfis de usuário móveis entre os dois tipos pode levar a inconsistências nas propriedades do perfil quando um usuário se move entre eles.

## Configurações de política de Redirecionamento de Arquivos

A seção **Redirecionamento de Arquivos** inclui configurações de política relacionadas ao mapeamento de unidades cliente e otimização de unidades cliente.

### Conectar automaticamente unidades cliente

Esta configuração permite ou impede a conexão automática de unidades cliente quando os usuários fazem logon.

Por padrão, a conexão automática é permitida.

Ao adicionar esta configuração a uma política, certifique-se de habilitar as configurações para os tipos de unidade que você deseja conectar automaticamente. Por exemplo, para permitir a conexão automática das unidades de CD-ROM dos usuários, configure esta configuração e a configuração **Unidades ópticas cliente**.

As seguintes configurações de política estão relacionadas:

- **Redirecionamento de unidade cliente**
- **Unidades de disquete cliente**
- **Unidades ópticas cliente**
- **Unidades fixas cliente**
- **Unidades de rede cliente**
- **Unidades removíveis cliente**

### Redirecionamento de unidade cliente

Esta configuração habilita ou desabilita o redirecionamento de arquivos para e de unidades no dispositivo do usuário.

Por padrão, o redirecionamento de arquivos está habilitado.

> **Nota:**

> As configurações de política de redirecionamento de unidade cliente não se aplicam a unidades mapeadas para sessões usando redirecionamento USB genérico.

> Quando habilitado, os usuários podem salvar arquivos em todas as suas unidades cliente. Quando desabilitado, todo o redirecionamento de arquivos é impedido. Esta configuração é

> aplicável independentemente do estado das configurações individuais de redirecionamento de arquivos. As configurações individuais de redirecionamento de arquivos incluem unidades de disquete cliente e unidades de rede cliente.

As seguintes configurações de política estão relacionadas:

- **Unidades de disquete cliente**
- **Unidades ópticas cliente**
- **Unidades fixas cliente**
- **Unidades de rede cliente**
- **Unidades removíveis cliente**

### Unidades fixas cliente

Essa configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades fixas no dispositivo do usuário.

Por padrão, o acesso a unidades fixas cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades fixas cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente, independentemente do estado da configuração **Unidades fixas cliente**.

Configure a configuração **Conectar unidades cliente automaticamente** para garantir que as unidades fixas sejam conectadas automaticamente quando os usuários fizerem logon.

### Unidades de disquete do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades de disquete no dispositivo do usuário.

Por padrão, o acesso a unidades de disquete do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades de disquete do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente, independentemente do estado da configuração **Unidades de disquete do cliente**.

Para garantir que as unidades de disquete sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades do cliente automaticamente**.

### Unidades de rede do cliente

Esta configuração permite ou impede que os usuários acessem e salvem arquivos em unidades de rede (remotas) através do dispositivo do usuário.

Por padrão, o acesso a unidades de rede do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades de rede do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Esta configuração é aplicável independentemente do estado da configuração **Unidades de rede do cliente**.

Para garantir que as unidades de rede sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades do cliente automaticamente**.

### Unidades ópticas do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos nos seguintes locais:

- CD-ROM no dispositivo do usuário
- DVD-ROM no dispositivo do usuário
- Unidades BD-ROM no dispositivo do usuário.

Por padrão, o acesso a unidades ópticas do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja presente e definida como **Permitido**. Se essas configurações estiverem desabilitadas, as unidades ópticas do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Esta configuração é aplicável independentemente do estado da configuração **Unidades ópticas do cliente**.

Para garantir que as unidades ópticas sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades cliente automaticamente**.

### Unidades removíveis do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades USB no dispositivo do usuário.

Por padrão, o acesso a unidades removíveis do cliente é permitido.

Ao adicionar esta configuração a uma política, verifique se a configuração **Redirecionamento de unidade cliente** está presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades removíveis do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Esta configuração é aplicável independentemente do estado da configuração **Unidades removíveis do cliente**.

Configure a configuração **Conectar unidades cliente automaticamente** para garantir que as unidades removíveis sejam conectadas automaticamente quando os usuários fizerem logon.

**Redirecionamento do host para o cliente**

Esta configuração habilita ou desabilita associações de tipo de arquivo para URLs e alguns conteúdos de mídia a serem abertos no dispositivo do usuário. Quando desabilitado, o conteúdo é aberto no servidor.

Por padrão, a associação de tipo de arquivo está desabilitada.

Estes tipos de URL são abertos localmente quando você habilita esta configuração:

- HTTP
- HTTPS
- Real Player e QuickTime (RTSP)
- Real Player e QuickTime (RTSPU)
- Real Player Legado (PNM)
- Microsoft Media Server (MMS)

**Preservar letras de unidade do cliente**

Essa configuração habilita ou desabilita o mapeamento de unidades do cliente para a mesma letra de unidade na sessão.

Por padrão, as letras de unidade do cliente não são preservadas.

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido.

**Acesso somente leitura à unidade do cliente**

Essa configuração permite ou impede que usuários e aplicativos façam o seguinte:

- Criar arquivos em unidades de cliente mapeadas

- Alterar arquivos em unidades de cliente mapeadas
- Alterar pastas em unidades de cliente mapeadas

Por padrão, arquivos e pastas em unidades de cliente mapeadas podem ser alterados.

Se definido como Habilitado, arquivos e pastas são acessíveis com permissões somente leitura.

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido.

**Redirecionamento de pasta especial**

Essa configuração permite ou impede que usuários do aplicativo Citrix Workspace™ e da Web Interface vejam suas pastas especiais locais de Documentos e Área de Trabalho a partir de uma sessão.

Por padrão, o redirecionamento de pasta especial é permitido.

Esta configuração impede que quaisquer objetos filtrados por meio de uma política tenham redirecionamento de pasta especial, independentemente das configurações existentes em outros lugares. Quando esta configuração é proibida, quaisquer configurações relacionadas especificadas para StoreFront™, Web Interface ou Citrix Workspace app são ignoradas.

Para definir quais usuários podem ter redirecionamento de pasta especial, selecione **Permitido** e inclua esta configuração em uma política filtrada nos usuários que você deseja que tenham esse recurso. Esta configuração substitui todas as outras configurações de redirecionamento de pasta especial.

As configurações de política que impedem os usuários de acessar ou salvar arquivos em seus discos rígidos locais também impedem o funcionamento do redirecionamento de pasta especial. Essa situação ocorre porque o redirecionamento de pasta especial deve interagir com o dispositivo do usuário.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Unidades fixas do cliente** esteja presente e definida como Permitido.

**Políticas de transferência de arquivos**

Por padrão, a transferência de arquivos está habilitada. Use o Web Studio para alterar essas políticas, localizadas em **Configuração do usuário - ICA\Redirecionamento de arquivos**. Considere o seguinte ao usar políticas de transferência de arquivos:

- **Transferência de arquivos para Citrix Workspace app para Chrome OS/HTML5** - Permite ou impede que os usuários transfiram arquivos entre uma sessão do Citrix Virtual Apps and Desktops e seus dispositivos.
- **Upload de arquivo para Citrix Workspace app para Chrome OS/HTML5** - Permite ou impede que os usuários carreguem arquivos de seus dispositivos para uma sessão do Citrix Virtual Apps and Desktops.
- **Download de arquivo para Citrix Workspace app para Chrome OS/HTML5** - Permite ou impede que os usuários baixem arquivos de uma sessão do Citrix Virtual Apps and Desktops para seus dispositivos.

> **Observação:**
>
> As políticas de transferência de arquivos são aplicáveis apenas para o Citrix Workspace app para HTML5 e para o Citrix Workspace app para Chrome OS.

**Usar gravações assíncronas**

Esta configuração habilita ou desabilita gravações assíncronas em disco.

Por padrão, as gravações assíncronas estão desabilitadas.

As gravações assíncronas em disco podem melhorar a velocidade das transferências de arquivos e da gravação em discos de cliente em WANs, que são tipicamente caracterizadas por largura de banda relativamente alta e alta latência. No entanto, se houver uma falha de conexão ou de disco, o arquivo ou arquivos do cliente que estão sendo gravados podem terminar em um estado indefinido. Se esse estado indefinido ocorrer, uma janela pop-up informa o usuário sobre os arquivos afetados. O usuário pode então tomar medidas corretivas, como reiniciar uma transferência de arquivo interrompida na reconexão ou quando a falha do disco for corrigida.

A Citrix® recomenda habilitar gravações assíncronas em disco apenas para usuários que exigem conectividade remota com boa velocidade de acesso a arquivos. E que podem recuperar facilmente arquivos ou dados perdidos em caso de falha de conexão ou de disco.

Ao adicionar esta configuração a uma política, verifique se a configuração **Redirecionamento de unidade do cliente** está presente e definida como Permitido. Se esta configuração estiver desativada, as gravações assíncronas não ocorrerão.

## Configurações de política de gráficos

A seção **Gráficos** inclui configurações de política para controlar como as imagens são tratadas nas sessões do usuário.

### Permitir compressão visualmente sem perdas

Esta configuração permite que a compressão visualmente sem perdas seja usada em vez da compressão verdadeiramente sem perdas para gráficos. A compressão visualmente sem perdas melhora o desempenho em relação à verdadeiramente sem perdas, mas tem uma pequena perda que é imperceptível à vista. Esta configuração altera a forma como os valores da configuração de Qualidade visual são usados.

Por padrão, esta configuração está desabilitada.

### Indicador de status de gráficos

Esta configuração configura o indicador de status de gráficos para ser executado na sessão do usuário. Esta ferramenta permite que o usuário veja informações sobre o modo gráfico ativo. As informações incluem detalhes sobre codec de vídeo, codificação de hardware, qualidade de imagem e monitores em uso para a sessão. Com o indicador de status de gráficos, o usuário também pode habilitar ou desabilitar o modo pixel-perfect.

As versões do Citrix Virtual Apps and Desktops™ 2103 e posteriores incluem um controle deslizante de qualidade de imagem para ajudar o usuário a encontrar o equilíbrio certo entre qualidade de imagem e interatividade.

As versões do Citrix Virtual Apps and Desktops 2109 e posteriores incluem funcionalidade para configurar um layout de exibição virtual por meio de uma interface de usuário iniciada usando o indicador de status de gráficos.

O indicador de status de gráficos substitui a ferramenta de indicador sem perdas de versões anteriores. Esta política habilita o indicador sem perdas para as versões 7.16 a 1809 do Citrix Virtual Apps and Desktops.

### Compartilhamento de tela

Esta configuração permite que os usuários compartilhem suas sessões, incluindo conteúdo da tela, teclados e mouses, com outros usuários.

Por padrão, a configuração está desabilitada.

O VDA tenta usar portas do intervalo de portas TCP para trocar dados, começando com a porta mais baixa e incrementando a cada conexão subsequente. A porta lida com tráfego de entrada e saída.

Por padrão, o intervalo de portas TCP é definido como 52525-52625.

A porta usada para compartilhamento de tela deve ser adicionada à lista de exceções do firewall. Esta opção é mostrada como uma caixa de seleção ao instalar o VDA. Por padrão, esta opção não está marcada.

**Limite de memória de exibição**

Esta configuração especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão.

Por padrão, o limite de memória de exibição é de 65.536 kilobytes.

Especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão. Especifique um valor em kilobytes de 128 a 4.194.303. O valor máximo de 4.194.303 não limita a memória de exibição. Por padrão, a memória de exibição é de 65.536 kilobytes. Usar mais profundidade de cor e maior resolução para conexões requer mais memória. No modo gráfico legado, se o limite de memória for atingido, a exibição degrada de acordo com a configuração "Preferência de degradação do modo de exibição".

Para conexões que exigem maior profundidade de cor e maior resolução, aumente o limite. Calcule a memória máxima necessária usando a equação:

Profundidade da memória em bytes = (profundidade-de-cor-em-bits-por-pixel) / 8) x (resolução-vertical-em-pixels) x (resolução-horizontal-em-pixels).

Por exemplo, considere um cenário com profundidade de cor de 32, resolução vertical de 600 e resolução horizontal de 800. Neste caso, a memória máxima necessária é (32 / 8) x (600) x (800) = 1920000 bytes, o que resulta em um limite de memória de exibição de 1920 KB.

Profundidades de cor diferentes de 32 bits estão disponíveis apenas se a configuração de política do modo gráfico legado estiver ativada.

O HDX™ aloca apenas a quantidade de memória de exibição necessária para cada sessão. Assim, se apenas alguns usuários exigirem mais do que o padrão, não haverá impacto negativo na escalabilidade ao aumentar o limite de memória de exibição.

**Preferência de degradação do modo de exibição**

> **Observação:**

> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica apenas quando a configuração de política do modo gráfico legado está ativada.

> Quando o limite de memória de exibição da sessão é atingido, esta configuração especifica se a profundidade de cor ou a resolução degrada primeiro.

Por padrão, a profundidade de cor é degradada primeiro.

Quando o limite de memória da sessão é atingido, você pode reduzir a qualidade das imagens exibidas. Você pode reduzir essa qualidade escolhendo se a profundidade de cor ou a resolução é degradada primeiro. Quando a profundidade de cor é degradada primeiro, as imagens exibidas usam menos cores. Quando a resolução é degradada primeiro, as imagens exibidas usam menos pixels por polegada.

Para notificar os usuários quando a profundidade de cor ou a resolução for degradada, configure a definição Notificar usuário quando o modo de exibição for degradado.

**Visualização dinâmica de janelas**

Esta configuração ativa ou desativa a exibição de janelas contínuas em:

- Flip-
- Flip 3D
- Visualização da barra de tarefas
- Windows Peek

| OPÇÃO DE VISUALIZAÇÃO DO WINDOWS AERO | DESCRIÇÃO |
|---|---|
| Visualização da Barra de Tarefas | Quando o usuário passa o mouse sobre o ícone da barra de tarefas de uma janela, uma imagem dessa janela aparece acima da barra de tarefas. |
| Windows Peek | Quando o usuário passa o mouse sobre uma imagem de visualização da barra de tarefas, uma imagem em tamanho real da janela aparece na tela. |

| OPÇÃO DE VISUALIZAÇÃO DO WINDOWS AERO | DESCRIÇÃO |
| --- | --- |
| Flip | Quando o usuário pressiona ALT+TAB, pequenos ícones de visualização são mostrados para cada janela aberta. |
| Flip 3D | Quando o usuário pressiona a tecla TAB+logotipo do Windows, imagens grandes das janelas abertas são exibidas em cascata na tela. |

Por padrão, esta configuração está habilitada.

### Cache de imagem

> **Observação:**
>
> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

Esta configuração habilita ou desabilita o armazenamento em cache e a recuperação de seções de imagens em sessões. O armazenamento em cache de imagens em seções e a recuperação dessas seções quando necessário proporciona o seguinte:

- Rolagem mais suave no dispositivo do usuário
- Reduz a quantidade de dados transmitidos pela rede no dispositivo do usuário
- Reduz o processamento necessário no dispositivo do usuário

Por padrão, a configuração de cache de imagem está ativada.

> **Observação:**
>
> A configuração de cache de imagem controla como as imagens são armazenadas em cache e recuperadas. A configuração não controla se as imagens são armazenadas em cache. As imagens são armazenadas em cache se a configuração de modo gráfico herdado estiver habilitada.

**Modo gráfico herdado - não suportado. Apenas para compatibilidade com versões anteriores**

> **Importante:**
>
> Não oferecemos suporte ao modo gráfico herdado e ao Redirecionamento de Composição da Área de Trabalho (DCR) nesta versão. Esta política é incluída apenas para compatibilidade com versões anteriores ao usar XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores do VDA com Windows 7 e Windows 2008 R2.

> Esta configuração desabilita a experiência gráfica rica. Use esta configuração para reverter para a experiência gráfica herdada, reduzindo o consumo de largura de banda em uma conexão WAN ou móvel. As reduções de largura de banda introduzidas no XenApp e XenDesktop 7.13 tornam este modo obsoleto.

Por padrão, esta configuração está desabilitada e os usuários recebem a experiência gráfica rica.

O modo gráfico herdado é compatível com o seguinte:

- Windows 7
- VDAs do Windows Server 2008 R2.

O modo gráfico herdado não é compatível com o seguinte:

- Windows 8.x e 10
- Windows Server 2012, 2012 R2 e 2016.

Consulte CTX202687 para obter mais informações sobre como otimizar modos gráficos e políticas no XenApp e XenDesktop 7.6 FP3 ou superior.

**Profundidade de cor máxima permitida**

> **Observação:**
>
> Para o Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

> Essa configuração especifica a profundidade de cor máxima permitida para uma sessão.

Por padrão, a profundidade de cor máxima permitida é de 32 bits por pixel.

Essa configuração se aplica apenas a drivers e conexões Thinwire. Ela não se aplica a VDAs que têm um driver não ThinWire como driver de exibição principal. Esses VDAs são VDAs que usam um driver Windows Display Driver Model (WDDM) como driver de exibição principal. Para VDAs de SO de sessão única que usam um driver WDDM como driver de exibição principal, como o Windows 8, essa configuração não tem efeito. Para VDAs de SO multissessão do Windows que usam um driver WDDM, como o Windows Server 2012 R2, essa configuração pode impedir que os usuários se conectem ao VDA.

Definir uma alta profundidade de cor requer mais memória. Para degradar a profundidade de cor quando o limite de memória for atingido, configure a configuração **Preferência de degradação do modo de exibição**. Quando a profundidade de cor é degradada, as imagens exibidas usam menos cores.

**Notificar o usuário quando o modo de exibição for degradado**

> **Observação:**
>
> Para o Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.
>
> Essa configuração exibe uma breve explicação ao usuário quando a profundidade de cor ou a resolução é degradada.

Por padrão, a notificação de usuários está desabilitada.

**Otimizar para carga de trabalho de gráficos 3D**

Essa configuração define as configurações padrão apropriadas que melhor se adequam a cargas de trabalho graficamente intensas. Habilite essa configuração para usuários cuja carga de trabalho se concentra em aplicativos graficamente intensos. Aplique essa política somente em casos em que uma GPU esteja disponível para a sessão. Quaisquer outras configurações que substituam explicitamente as configurações padrão definidas por essa política terão precedência.

Por padrão, a otimização para a carga de trabalho de gráficos 3D está desativada.

**Enfileiramento e descarte**

> **Observação:**

> Para o Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

> Essa configuração descarta imagens enfileiradas que são substituídas por outra imagem.

Por padrão, o enfileiramento e descarte está habilitado.

Essa configuração melhora a resposta quando os gráficos são enviados para o dispositivo do usuário. A configuração dessa opção pode fazer com que as animações fiquem instáveis devido a quadros perdidos.

**Usar codec de vídeo para compactação**

Permite o uso de um codec de vídeo para compactar gráficos quando a decodificação de vídeo está disponível no endpoint. Quando **Para a tela inteira** é escolhido, o codec de vídeo é aplicado como o codec padrão para todos. Quando **Para regiões em constante mudança** é selecionado, o codec de vídeo é usado para áreas onde há mudança constante na tela; outros dados usam compactação de imagem estática e cache de bitmap. Quando a decodificação de vídeo não está disponível no endpoint, ou quando você especifica **Não usar codec de vídeo**, uma combinação de compactação de imagem estática e cache de bitmap é usada. Quando **Usar quando preferencial** é selecionado, o sistema escolhe, com base em vários fatores. Os resultados podem variar entre as versões à medida que o método de seleção é aprimorado.

Selecione **Usar quando preferencial** para permitir que o sistema faça o seu melhor para escolher as configurações apropriadas para o cenário atual.

Selecione **Para a tela inteira** para otimizar a experiência do usuário e a largura de banda, especialmente em casos de uso intenso de vídeo renderizado por servidor e gráficos 3D.

Selecione **Para regiões em constante mudança** para otimizar o desempenho de vídeo, especialmente em baixa largura de banda, mantendo a escalabilidade para conteúdo estático e de mudança lenta. Essa configuração é suportada em implantações com vários monitores.

Selecione **Não usar codec de vídeo** para otimizar a carga da CPU do servidor e para casos que não possuem muitos vídeos renderizados por servidor ou outros aplicativos graficamente intensos.

O padrão é **Usar quando preferencial**.

### Usar codificação de hardware para vídeo

Esta configuração permite o uso de hardware gráfico, se disponível, para compactar elementos da tela com o codec de vídeo. Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software.

A opção padrão para esta configuração de política é **Habilitado**.

Vários monitores são suportados.

Qualquer aplicativo Citrix Workspace™ que suporte decodificação de vídeo pode ser usado com codificação de hardware.

#### NVIDIA

Para GPUs NVIDIA GRID, a codificação de hardware é suportada com VDAs para SO Multi-sessão e SO de Sessão Única.

As GPUs NVIDIA devem suportar a codificação de hardware NVENC. Consulte NVIDIA video codec SDK para obter uma lista de GPUs suportadas.

NVIDIA GRID requer a versão de driver 3.1 ou superior. NVIDIA Quadro requer a versão de driver 362.56 ou superior. A Citrix recomenda drivers do branch NVIDIA Release R361.

O texto sem perdas não é compatível com a codificação de hardware NVENC. Se você ativou o texto sem perdas, o texto sem perdas tem prioridade sobre a codificação de hardware NVENC.

O uso seletivo do codec de hardware H.264 para regiões em constante mudança é suportado.

A compressão visualmente sem perdas (YUV 4:4:4) é suportada. Visualmente sem perdas (configuração de política gráfica, Permitir compressão visualmente sem perdas) requer Citrix Workspace app 1808 ou superior ou Citrix Receiver para Windows 4.5 ou superior.

#### INTEL

Para processadores gráficos Intel Iris Pro, a codificação de hardware é suportada com VDAs para SO de Sessão Única e SO Multi-sessão.

Os processadores gráficos Intel Iris Pro da família de processadores Intel Broadwell e posteriores são suportados. A versão 1.0 do Intel Remote Displays SDK é necessária e pode ser baixada do site da Intel: Remote Displays SDK.

O texto sem perdas é suportado apenas quando a política de codec de vídeo é definida para a tela inteira e a política **Otimizar para carga de trabalho de gráficos 3D** está desabilitada.

Sem perdas visuais (YUV 4:4:4) não é suportado.

O codificador Intel oferece uma boa experiência de usuário para até oito sessões de codificação (por exemplo, um usuário usando oito monitores ou oito usuários usando um monitor cada). Se mais de oito sessões de codificação forem necessárias, verifique quantos monitores a máquina virtual se conecta. O administrador decide configurar esta política por usuário ou por máquina para manter uma boa experiência de usuário.

#### AMD

Para AMD, a codificação de hardware é suportada com VDAs para um SO de sessão única.

As GPUs AMD devem suportar o SDK RapidFire. Por exemplo, as GPUs AMD Radeon Pro ou FirePro.

Para que a codificação funcione, instale os drivers AMD mais recentes. Você pode baixar esses drivers em `<https://www.amd.com/en/support>`.

O texto sem perdas não é compatível com a codificação de hardware AMD. Se você ativou o texto sem perdas, o texto sem perdas tem prioridade sobre a codificação de hardware AMD.

O uso seletivo do codec de hardware H.264 para regiões em constante mudança é suportado.

## Configurações de política de keep-alive

A seção **Keep Alive** contém configurações de política para gerenciar mensagens ICA® keep-alive.

### Tempo limite de keep-alive do ICA

Esta configuração especifica o número de segundos entre mensagens ICA keep-alive sucessivas.

Por padrão, o intervalo entre as mensagens keep-alive é de 60 segundos.

Especifique um intervalo entre 1 e 3600 segundos para enviar mensagens ICA keep-alive. Não configure esta definição se o seu software de monitorização de rede for responsável por fechar ligações inativas.

### Mensagens ICA keep-alive

Esta configuração ativa ou desativa o envio periódico de mensagens ICA keep-alive.

Por padrão, as mensagens keep-alive não são enviadas.

A ativação desta configuração impede que conexões quebradas sejam desconectadas. Se o servidor não detectar atividade, esta configuração impede que os Serviços de Área de Trabalho Remota (RDS) desconectem a sessão. O servidor envia mensagens keep-alive a cada poucos

segundos para detectar se a sessão está ativa. Se a sessão não estiver mais ativa, o servidor a marca como desconectada.

O ICA keep-alive não funciona se você estiver usando a confiabilidade da sessão. Configure o ICA keep-alive apenas para conexões que não estão usando a Confiabilidade da Sessão.

Configurações de política relacionadas: Conexões de confiabilidade da sessão.

## Configurações de política de multimídia

A seção **Multimídia** inclui configurações de política para gerenciar streaming de áudio e vídeo HTML5 e Windows em sessões de usuário.

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

### Políticas de multimídia

Por padrão, todas as políticas de multimídia definidas no Delivery Controller™ são armazenadas nestes registros:

Políticas de máquina:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

Políticas de usuário:

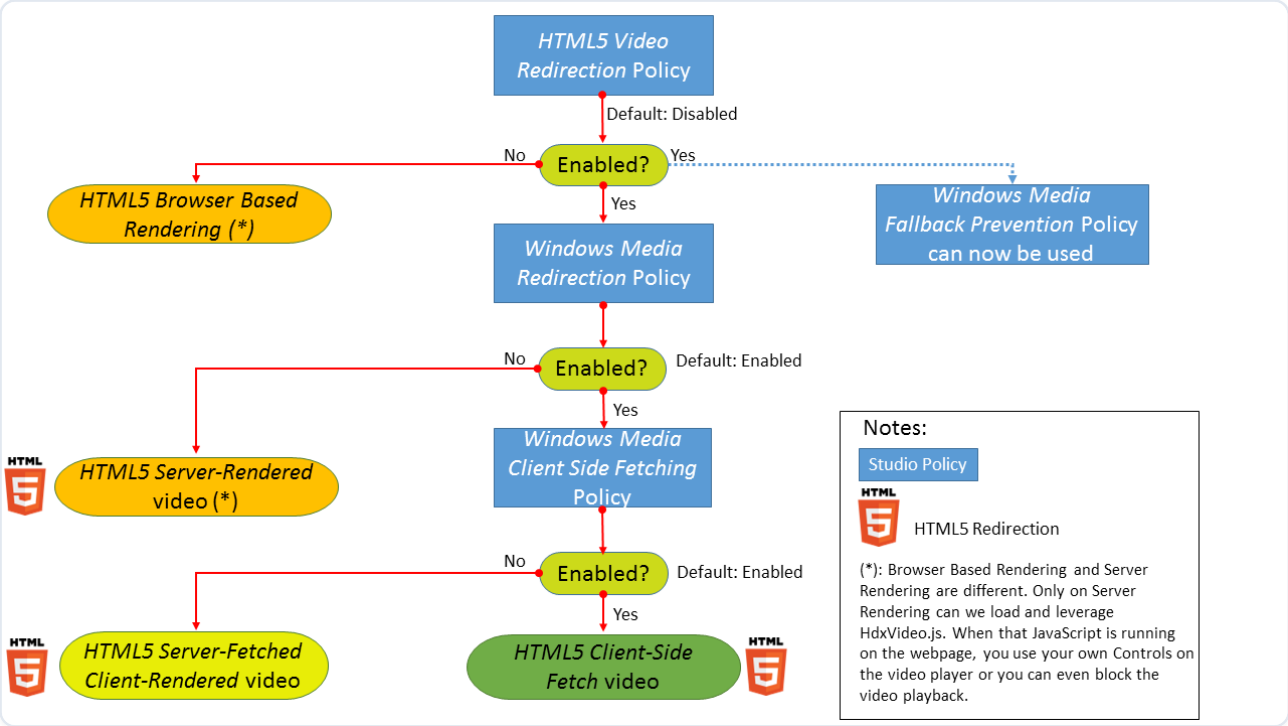
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

Para localizar o ID da sessão do usuário atual, execute o comando **qwinsta** na linha de comando do Windows.

### Redirecionamento de vídeo HTML5

Controla e otimiza a forma como os servidores Citrix Virtual Apps and Desktops™ entregam conteúdo web multimídia HTML5 aos usuários.

Por padrão, esta configuração está desabilitada.




Nesta versão, este recurso está disponível apenas para páginas da web controladas. Requer a adição de JavaScript às páginas da web onde o conteúdo multimídia HTML5 está disponível, por exemplo, vídeos em um site de treinamento interno.

Para configurar o redirecionamento de vídeo HTML5:

1. Copie o arquivo, **HdxVideo.js**, de %Program Files%/Citrix/ICA Service/HTML5 Video Redirection na instalação do VDA para o local da sua página da web interna.
2. Insira esta linha em sua página da web (se sua página da web tiver outros scripts, inclua **HdxVideo.js** antes desses scripts): `<script src="HdxVideo.js" type="text/javascript"\></script>`

**Nota:** Se HdxVideo.js não estiver no mesmo local que sua página da web, use o atributo **src** para especificar o caminho completo para ele.

Considere que o JavaScript não é adicionado às suas páginas da web controladas e o usuário reproduz um vídeo HTML5. Neste caso, o Citrix Virtual Apps and Desktops assume como padrão a renderização do lado do servidor.

Para que o redirecionamento de vídeos HTML5 funcione, permita ***Redirecionamento de Mídia do Windows***. Esta política é obrigatória para Server Fetch Client Render e necessária para Client Side Fetching. Client Side Fetching, por sua vez, também requer que *a busca de conteúdo do lado do cliente do Windows Media* seja Permitida.

O Microsoft Edge não oferece suporte a este recurso.

HdxVideo.js substitui os controles do Player HTML5 do navegador pelos seus próprios. Para verificar se a política de redirecionamento de vídeo HTML5 está em vigor em um determinado site, compare os controles do player com um cenário onde a política de **redirecionamento de vídeo HTML5** é Proibida:

(Controles personalizados do Citrix quando a política é Permitida)



(Controles nativos da página da web quando a política é Proibida ou não configurada)




Os seguintes controles de vídeo são suportados:

- reproduzir
- pausa
- buscar
- repetir
- áudio
- tela cheia

Você pode visualizar uma página de teste de redirecionamento de vídeo HTML5.

### TLS, REDIRECIONAMENTO DE VÍDEO HTML5 E REDIRECIONAMENTO DE CONTEÚDO DO NAVEGADOR

Você pode usar o redirecionamento de vídeo HTML5 para:

- Redirecionar vídeos de sites HTTPS
- Ou
- Redirecionamento de conteúdo do navegador para redirecionar o site inteiro

O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) em execução no VDA. O Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX no armazenamento de certificados no VDA gera dois certificados personalizados para:

- Realizar o redirecionamento de vídeo
- Manter a integridade TLS da página da web

HdxVideo.js usa WebSockets Seguros para se comunicar com o WebSocketService.exe em execução no VDA. Este processo é executado como uma conta de Sistema Local e faz a terminação SSL e o mapeamento de sessão do usuário.

WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

**Limitar a qualidade do vídeo**

Esta configuração se aplica apenas ao Windows Media e não ao HTML5. Ela exige que você ative a **Otimização para redirecionamento multimídia do Windows Media em WAN**.

Esta configuração especifica o nível máximo de qualidade de vídeo permitido para uma conexão HDX™. Quando configurada, a qualidade máxima do vídeo é limitada ao valor especificado, garantindo que a Qualidade de Serviço (QoS) multimídia seja mantida em um ambiente.

Por padrão, esta configuração não está configurada.

Para limitar o nível máximo de qualidade de vídeo permitido, escolha uma das seguintes opções:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Reproduzir vários vídeos simultaneamente no mesmo servidor consome grandes quantidades de recursos e pode afetar a escalabilidade do servidor.

**Redirecionamento do Microsoft Teams**

Esta configuração permite a otimização do Microsoft Teams, com base na tecnologia HDX.

Se esta política estiver ativada e você estiver usando uma versão compatível do aplicativo Citrix Workspace™, esta chave de registro é definida como **1** no VDA. O aplicativo Microsoft Teams lê a chave para carregar no modo VDI. Observe que não é necessário definir a chave de registro manualmente.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Nome: MSTeamsRedirSupport

Valor: DWORD (1 - ativado, 0 - desativado)

> **Nota:**
>
> Considere que você está usando VDAs versão 1906.2 ou posterior com versões mais antigas do Controller, que não têm a política disponível no Web Studio. Um exemplo de uma versão mais antiga do Controller é a versão 7.15. Neste caso, a otimização HDX é habilitada por padrão no VDA. Se a versão do aplicativo Workspace for 1907 ou posterior, o Microsoft Teams será iniciado no modo otimizado. Para obter informações sobre ressalvas na mistura de Controllers 7.15 LTSR e VDAs CR, consulte o artigo do Knowledge Center CTX205549.

> Neste caso, para desabilitar o recurso para usuários específicos, você pode substituir a configuração do registro. Substitua as configurações do registro usando uma política de grupo para aplicar um script de logon à unidade organizacional do usuário.

> Por padrão, o redirecionamento do Microsoft Teams está habilitado.

**Conferência multimídia**

Essa configuração permite ou impede o uso da tecnologia de redirecionamento otimizado de webcam por aplicativos de videoconferência.

Por padrão, o suporte a videoconferência é permitido.

Ao adicionar essa configuração a uma política, verifique se a configuração de **redirecionamento do Windows Media** está presente e definida como **Permitido** (o padrão).

Ao usar a **conferência multimídia**, verifique se as seguintes condições são atendidas:

- Os drivers fornecidos pelo fabricante para a webcam usada para conferência multimídia estão instalados no cliente.
- Conecte a webcam ao dispositivo do usuário antes de iniciar uma sessão de videoconferência. O servidor usa apenas uma webcam instalada por vez. Se várias webcams estiverem instaladas no dispositivo do usuário, o servidor tentará usar cada webcam em sucessão. Essa tentativa continua até que uma sessão de videoconferência seja criada com sucesso.

Essa política não é necessária ao redirecionar a webcam usando o redirecionamento USB genérico. Nesse caso, instale os drivers da webcam no VDA.

### Otimização para redirecionamento multimídia do Windows Media sobre WAN

Essa configuração se aplica apenas ao Windows Media e não ao HTML5. A configuração permite o seguinte:

- Transcodificação multimídia em tempo real
- Permite o streaming de mídia de áudio e vídeo para dispositivos móveis em redes degradadas
- Melhora a experiência do usuário ao aprimorar a forma como o conteúdo do Windows Media é entregue por uma WAN.

Por padrão, a entrega de conteúdo do Windows Media pela WAN é otimizada.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de Mídia do Windows** esteja presente e definida como **Permitido**.

Quando esta configuração está ativada, a transcodificação multimídia em tempo real é implantada automaticamente conforme necessário para permitir o streaming de mídia. Além disso, proporciona uma experiência de usuário perfeita mesmo em condições de rede extremas.

### Usar GPU para otimizar o redirecionamento multimídia do Windows Media pela WAN

Esta configuração se aplica apenas ao Windows Media e permite que a transcodificação multimídia em tempo real seja feita na Unidade de Processamento Gráfico (GPU) no Virtual Delivery Agent (VDA). Ela melhora a escalabilidade do servidor. A transcodificação por GPU está disponível apenas se o VDA tiver uma GPU compatível para aceleração de hardware. Caso contrário, a transcodificação retorna à CPU.

**Nota:** A transcodificação por GPU é suportada apenas em GPUs NVIDIA.

Por padrão, o uso da GPU no VDA para otimizar a entrega de conteúdo do Windows Media pela WAN é proibido.

Ao adicionar esta configuração a uma política, certifique-se de que as seguintes configurações estejam presentes e definidas como Permitido:

- **Redirecionamento de Mídia do Windows**
- **Otimização para configurações de redirecionamento multimídia do Windows Media pela WAN**

### Prevenção de fallback do Windows Media

Esta configuração se aplica à redireção de conteúdo do navegador, HTML5 e Windows Media. Para que ela suporte HTML5, defina a política de **redirecionamento de vídeo HTML5** como **Permitido**.

Os administradores podem usar a configuração de política **Prevenção de fallback do Windows Media** para especificar os métodos que são tentados para entregar conteúdo transmitido aos usuários.

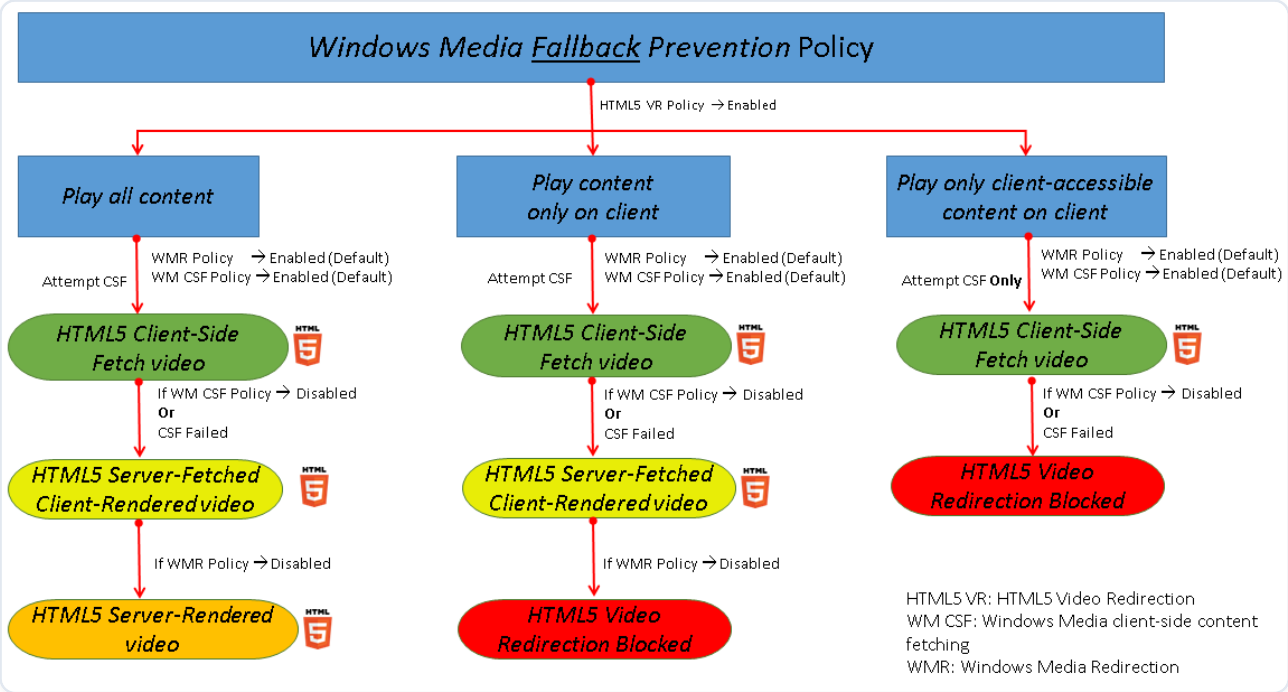
Por padrão, essa configuração não está configurada. Quando a configuração é definida como Não Configurado, o comportamento é o mesmo que **Reproduzir todo o conteúdo**.

Para configurar essa definição, escolha uma das seguintes opções:

- **Reproduzir todo o conteúdo**. Tentar buscar conteúdo do lado do cliente, depois Redirecionamento do Windows Media. Se não for bem-sucedido, reproduzir o conteúdo no servidor.
- **Reproduzir todo o conteúdo apenas no cliente**. Tentar buscar do lado do cliente, depois Redirecionamento do Windows Media. Se não for bem-sucedido, o conteúdo não será reproduzido.
- **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Tentar apenas buscar do lado do cliente. Se não for bem-sucedido, o conteúdo não será reproduzido.

Quando o conteúdo não é reproduzido, a seguinte mensagem de erro é exibida na janela do player (por uma duração padrão de 5 segundos):

```
"Company has blocked video because of lack of resources"
```




A duração desta mensagem de erro pode ser personalizada com a seguinte chave de registro no VDA. Se a entrada de registro não existir, a duração padrão será de 5 segundos.

O caminho do registro varia dependendo da arquitetura do VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

Ou

\HKLM\SOFTWARE\Citrix\HdxMediastream

Chave do Registro:

Nome: VideoLoadManagementErrDuration

Tipo: DWORD

Intervalo: 1 - até o limite de DWORD (padrão = 5)

Unidade: segundos

**Busca de conteúdo do lado do cliente do Windows Media**

Esta configuração se aplica tanto ao HTML5 quanto ao Windows Media. A configuração permite que um dispositivo de usuário transmita arquivos multimídia diretamente do provedor de origem na internet ou intranet, em vez de através do servidor host XenApp ou XenDesktop®.

Por padrão, esta configuração é **Permitida**. Permitir esta configuração melhora o uso da rede e a escalabilidade do servidor. Essa melhoria é alcançada movendo qualquer processamento de

mídia do servidor host para o dispositivo do usuário. Também remove a exigência de que uma estrutura multimídia avançada, como Microsoft DirectShow ou Media Foundation, seja instalada no dispositivo do usuário. O dispositivo do usuário requer apenas a capacidade de reproduzir um arquivo de uma URL

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento do Windows Media** esteja presente e definida como **Permitida**. Se o **Redirecionamento do Windows Media** estiver desabilitado, a transmissão de arquivos multimídia para o dispositivo do usuário diretamente do provedor de origem também será desabilitada.

**Redirecionamento do Windows Media**

Esta configuração se aplica tanto ao HTML5 quanto ao Windows Media e controla e otimiza a forma como os servidores entregam áudio e vídeo em streaming aos usuários.

Por padrão, esta configuração é **Permitida**. Para HTML5, esta configuração não tem efeito se a política **Redirecionamento de vídeo HTML5** for **Proibida**.

Quando esta configuração está habilitada, a qualidade do áudio e vídeo renderizados do servidor aumenta para um nível que se compara ao áudio e vídeo reproduzidos localmente em um dispositivo de usuário. O servidor transmite multimídia para o cliente na forma original e compactada e permite que o dispositivo do usuário descompacte e renderize a mídia.

O redirecionamento do Windows Media otimiza arquivos multimídia que são codificados com codecs que aderem aos padrões Microsoft DirectShow, DirectX Media Objects (DMO) e Media Foundation. Para reproduzir um determinado arquivo multimídia, um codec compatível com o formato de codificação do arquivo multimídia deve estar presente no dispositivo do usuário.

Por padrão, o áudio está desabilitado no aplicativo Citrix Workspace. Para permitir que os usuários executem aplicativos multimídia em sessões ICA®, ative o áudio ou dê aos usuários permissão para ativar o áudio na interface do aplicativo Citrix Workspace.

Selecione **Proibido** somente se a reprodução de mídia usando o redirecionamento do Windows Media parecer pior do que quando renderizada usando compressão ICA básica e áudio regular. Essa situação é rara, mas pode ocorrer em condições de baixa largura de banda, por exemplo, com mídia com baixa frequência de quadros-chave.

**Tamanho do buffer de redirecionamento do Windows Media**

Esta configuração é legada e não se aplica ao HTML5.

Esta configuração especifica um tamanho de buffer de 1 a 10 segundos para aceleração multimídia.

Por padrão, o tamanho do buffer é de 5 segundos.

#### Uso do tamanho do buffer de redirecionamento do Windows Media

Essa configuração é legada e não se aplica ao HTML5.

Essa configuração habilita ou desabilita o uso do tamanho do buffer especificado na configuração **Tamanho do buffer de redirecionamento do Windows Media**.

Por padrão, o tamanho do buffer especificado não é usado.

Se essa configuração estiver desabilitada ou se a configuração **Tamanho do buffer de redirecionamento do Windows Media** não estiver configurada, o servidor usará o valor padrão do tamanho do buffer (cinco segundos).

### Configurações de política de conexões multi-stream

A seção **Conexões Multi-Stream** inclui configurações de política para gerenciar a priorização de Qualidade de Serviço para múltiplas conexões ICA® em uma sessão.

> **Nota:**
>
> A Descoberta de MTU não é suportada se a política de conexões Multi-Stream estiver habilitada.

#### Áudio sobre UDP

Esta configuração permite ou impede o áudio sobre UDP no servidor.

Por padrão, o áudio sobre UDP é permitido no servidor.

Quando habilitada, esta configuração abre uma porta UDP no servidor para suportar todas as conexões configuradas para usar o Transporte em Tempo Real de Áudio sobre UDP.

#### Intervalo de portas UDP de áudio

Esta configuração especifica o intervalo de números de porta (número de porta mais baixo, número de porta mais alto) usado pelo Virtual Delivery Agent (VDA). Esta especificação ajuda a trocar dados de pacotes de áudio com o dispositivo do usuário. O VDA tenta usar cada par de portas UDP para trocar dados com o dispositivo do usuário, começando com o mais baixo e

incrementando em dois para cada tentativa subsequente. Cada porta lida com tráfego de entrada e saída.

Por padrão, este intervalo é definido como 16500,16509.

**Política Multi-Porta**

Esta configuração especifica as portas TCP a serem usadas para o tráfego ICA e estabelece a prioridade de rede para cada porta.

Por padrão, a porta primária (2598) tem prioridade Alta.

Ao configurar portas, você pode atribuir as seguintes prioridades:

- **Muito Alta:** para atividades em tempo real, como conferências por webcam
- **Alto:** para elementos interativos, como tela, teclado e mouse
- **Médio:** para processos em massa, como mapeamento de unidade cliente
- **Baixo:** para atividades em segundo plano, como impressão

Cada porta deve ter uma prioridade exclusiva. Por exemplo, você não pode atribuir uma prioridade Muito Alta às portas CGP 1 e CGP 3.

Para remover uma porta da priorização, defina o número da porta como 0. Você não pode remover a porta primária e não pode alterar seu nível de prioridade.

Ao configurar esta definição, reinicie o servidor. Esta definição só entra em vigor quando a definição de política **Multi-Stream computer** está ativada.

**Definição de computador Multi-Stream**

Esta definição ativa ou desativa o Multi-Stream no servidor.

Por padrão, o Multi-Stream está desativado. Configure a definição de política de computador Multi-Stream se você usar Citrix SD-WAN™ ou roteadores de terceiros para obter a Qualidade de Serviço desejada.

Se o Multi-Stream estiver ativado, o MTU Discovery, um recurso do Adaptive Transport, não é suportado.

Ao configurar essa definição, reinicie o servidor para garantir que as alterações entrem em vigor.

> **Importante:**

> Usar esta definição de política com definições de política de limite de largura de banda, como o limite geral de largura de banda da sessão, pode produzir resultados inesperados. Ao incluir esta definição em uma política, certifique-se de que as definições de limite de largura de banda não estejam incluídas.

### Definição de usuário Multi-Stream

Esta definição ativa ou desativa o Multi-Stream no dispositivo do usuário.

Por padrão, o Multi-Stream está desativado para todos os usuários. Configure a definição de usuário Multi-Stream se você usar Citrix SD-WAN ou roteadores de terceiros para obter a Qualidade de Serviço desejada.

Esta configuração só tem efeito em hosts onde a configuração de política **Computador Multi-Stream** está ativada.

> **Importante:**
>
> Usar esta configuração de política com configurações de política de limite de largura de banda, como Limite geral de largura de banda da sessão, pode produzir resultados inesperados. Ao incluir esta configuração em uma política, certifique-se de que as configurações de limite de largura de banda não estejam incluídas.

### Configurações de atribuição de canal virtual Multi-Stream

Esta configuração especifica o fluxo ICA ao qual os canais virtuais são atribuídos quando o multi-stream é usado.

Se você não configurar essas configurações, os canais virtuais serão mantidos em seu fluxo padrão. Para atribuir um canal virtual a um fluxo ICA, selecione o número do fluxo desejado (0, 1, 2, 3) na lista **Número do Fluxo** ao lado do nome do canal virtual.

Se houver um canal virtual personalizado em uso no ambiente, clique em **Adicionar**, especifique o nome do canal virtual na caixa de texto em **Canais Virtuais** e selecione o número do fluxo desejado na lista **Número do Fluxo** ao lado dele. O nome especificado deve ser o nome real do canal virtual e não um nome amigável. Por exemplo, CTXSBR em vez de Citrix Browser Acceleration.

Essas configurações só têm efeito quando você ativou a configuração de computador multi-stream.

Por padrão, os canais virtuais e suas atribuições de fluxo são:

- AppFlow®: 2
- Áudio: 0
- Redirecionamento de Conteúdo do Navegador: 2
- Mapeamento de Porta COM do Cliente: 3
- Mapeamento de Unidade do Cliente: 2
- Mapeamento de Impressora do Cliente: 3
- Área de Transferência: 2
- CTXDND: 1 (**Nota:** Isso suporta o arrastar e soltar arquivos entre uma sessão Citrix e um endpoint local.)
- Plug-in DVC (nome de VC estático gerado automaticamente a partir do Nome Amigável do Plug-in DVC, ou atribuído pelo administrador): 2
- Monitoramento da Experiência do Usuário Final: 1
- Transferência de Arquivos (HTML5 Receiver): 2
- Transferência Genérica de Dados: 2
- Controle ICA: 1
- Editor de Método de Entrada: 1
- Mapeamento de Impressora Cliente Legado (COM1): 1, 3
- Mapeamento de Impressora Cliente Legado (COM2): 2, 3
- Mapeamento de Impressora Cliente Legado (LPT1): 1, 3
- Mapeamento de Impressora Cliente Legado (LPT2): 2, 3
- Gerenciamento de Licenças: 1
- Redirecionamento do Microsoft Teams/WebRTC: 1
- Mobile Receiver: 1
- MultiTouch: 1
- Encaminhamento de Porta: 2
- Extensões Remotas de Áudio e Vídeo (RAVE): 2
- Seamless (Integração Transparente de Janelas): 1
- Sensor e Localização: 1
- Cartão Inteligente: 1

- Gráficos Thinwire: 1
- Integração Transparente da UI/Status de Logon: 2
- Redirecionamento TWAIN: 2
- USB: 2
- Fonte e Teclado de Latência Zero: 2
- Canal de Dados de Latência Zero: 2

Para obter mais informações sobre atribuições e prioridades de canais virtuais, consulte o artigo do Knowledge Center CTX131001.

## Configurações de política de redirecionamento de porta

A seção **Redirecionamento de Porta** contém configurações de política para mapeamento de porta LPT e COM do cliente.

Para versões do Virtual Delivery Agent **anteriores a 7.0**, use as seguintes configurações de política para configurar o redirecionamento de porta. Para as versões do VDA **7.0 a 7.8**, configure essas configurações usando o registro; consulte Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro. Para a versão do VDA **7.9**, use as seguintes configurações de política.

### Conectar automaticamente portas COM do cliente

Essa configuração habilita ou desabilita a conexão automática de portas COM em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas COM do cliente não são conectadas automaticamente.

### Conectar automaticamente portas LPT do cliente

Essa configuração habilita ou desabilita a conexão automática de portas LPT em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas LPT do cliente não são conectadas automaticamente.

### Redirecionamento de porta COM do cliente

Essa configuração permite ou impede o acesso às portas COM no dispositivo do usuário.

Por padrão, o redirecionamento de porta COM é proibido.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta COM

- Porcentagem de limite de largura de banda de redirecionamento de porta COM

#### Redirecionamento de porta LPT do cliente

Esta configuração permite ou impede o acesso às portas LPT no dispositivo do usuário.

Por padrão, o redirecionamento de porta LPT é proibido.

As portas LPT são usadas apenas por aplicativos legados que enviam trabalhos de impressão para as portas LPT. Essas portas não são usadas por aplicativos legados que enviam trabalhos de impressão para os objetos de impressão no dispositivo do usuário. A maioria dos aplicativos hoje pode enviar trabalhos de impressão para objetos de impressora. Esta configuração de política é necessária apenas para servidores que hospedam aplicativos legados que imprimem em portas LPT.

Observe que, embora o redirecionamento de porta COM do cliente seja bidirecional, o redirecionamento de porta LPT é apenas de saída e limitado a `\\client\LPT1` e `\\client\LPT2` dentro de uma sessão ICA.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta LPT
- Porcentagem de limite de largura de banda de redirecionamento de porta LPT

### Configurações de política de impressão

A seção Impressão contém configurações de política para gerenciar a impressão do cliente.

#### Redirecionamento de impressora cliente

Esta configuração controla se as impressoras cliente são mapeadas para um servidor quando um usuário faz logon em uma sessão.

Por padrão, o mapeamento de impressora cliente é permitido. Se esta configuração estiver desabilitada, a impressora PDF para a sessão não será criada automaticamente.

Configurações de política relacionadas: criar impressoras cliente automaticamente

#### Impressora padrão

Esta configuração especifica como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como impressora padrão para a sessão.

Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar a impressora padrão do usuário. Se você escolher esta opção, a impressora padrão não será salva no perfil e não mudará de acordo com outras propriedades de sessão ou cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é uma das seguintes:

- A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e **Impressoras**.
- A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

Você pode usar esta opção para apresentar aos usuários a impressora mais próxima por meio das configurações de perfil (conhecido como impressão por proximidade).

**Atribuições de impressora**

Esta configuração oferece uma alternativa às configurações de Impressora padrão e Impressoras de sessão. Use as configurações individuais de Impressora padrão e Impressoras de sessão para configurar comportamentos para um site, grupo grande ou unidade organizacional. Use a configuração **Atribuições de impressora** para atribuir um grande grupo de impressoras a vários usuários.

Esta configuração especifica como a impressora padrão nos dispositivos de usuário listados é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como a impressora padrão para a sessão.

Ele também especifica as impressoras de rede a serem criadas automaticamente em uma sessão para cada dispositivo de usuário. Por padrão, nenhuma impressora é especificada.

- Ao definir o valor da impressora padrão:

  Para usar a impressora padrão atual para o dispositivo de usuário, selecione Não ajustar.

  Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar. Se você escolher esta opção, a impressora padrão não será salva no perfil e não mudará de acordo com outras propriedades da sessão ou do cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é uma das seguintes:

  - A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e Impressoras.

    - A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

- Ao definir o valor das impressoras de sessão: para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Após adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual a cada logon.

**Preferência de log de eventos de criação automática de impressora**

Esta configuração especifica os eventos que são registrados durante o processo de criação automática de impressora. Você pode optar por não registrar erros ou avisos, apenas erros, ou erros e avisos.

Por padrão, erros e avisos são registrados.

Um exemplo de aviso é um evento em que o driver nativo de uma impressora não pode ser instalado e o driver de impressão universal é instalado em seu lugar. Para usar o driver de impressão universal neste cenário, configure a configuração de uso do driver de impressão universal para Usar somente impressão universal ou Usar somente impressão universal se o driver solicitado não estiver disponível.

**Impressoras de sessão**

Esta configuração especifica as impressoras de rede a serem criadas automaticamente em uma sessão. Dentro da sessão ICA/HDX, o serviço Citrix Print Manager (CpSvc.exe) cria uma conexão de impressora de rede durante o logon da sessão para cada impressora de rede especificada na configuração de política **Impressora de Sessão**. Ele exclui as impressoras durante o logoff da sessão. Por padrão, nenhuma impressora é especificada.

Na configuração de política **Session Printer**, as impressoras de rede podem residir em um Windows Print Server ou em um Citrix Universal™ Print Server.

- **Windows Print Server:** Compartilha uma ou mais impressoras de rede. Ele também possui os drivers de impressora nativos necessários para usar as impressoras de rede.
- **Universal Print Server:** Um Windows Print Server onde o software Citrix Universal Print Server foi instalado.

Ao usar um Windows Print Server, o serviço Citrix Print Manager cria as conexões de impressora de rede usando drivers de impressora nativos. O servidor Citrix Virtual Apps™ deve ter os drivers de impressora nativos instalados.

Ao usar um Citrix Universal Print Server, o serviço Citrix Print Manager cria as conexões de impressora de rede usando drivers de impressora nativos, Citrix Universal Printer Driver ou Citrix Universal XPS Printer Driver. O driver que você usa é controlado pela configuração de política de uso do Universal Print Driver.

Todos os drivers de impressora do Windows atualmente se enquadram nas versões de driver v3 ou v4. Para obter mais informações, consulte Suporte para as Arquiteturas de Driver de Impressora Microsoft V3 e V4.

Para adicionar impressoras de sessão e verificar se elas aparecem nas sessões, conclua o seguinte procedimento:

1. Faça login no Web Studio, selecione **Policies** no painel esquerdo e, em seguida, clique na guia **Policies**.
2. Habilite a política **Session printers**.
3. Na política, adicione a impressora de sessão. Para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Após adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual a cada logon. A impressora de sessão deve ser exibida na lista.
4. Depois que a política for definida, o aplicativo publicado pode não exibir as impressoras de sessão. Esse problema pode ocorrer porque o driver da impressora está ausente no servidor Citrix Virtual Apps ou a política foi criada, mas não habilitada.

   > **Observação:**
   >
   > Se uma impressora de sessão precisar de um driver de impressora nativo e o driver de impressora nativo não estiver instalado no VDA, a impressora de sessão poderá não ser criada na sessão.

5. Inicie a área de trabalho publicada e adicione manualmente a impressora de sessão em **Dispositivos e Impressoras > Painel de Controle**.
6. Se isso falhar, investigue a comunicação entre o servidor Citrix Virtual Apps e o servidor de impressão. Considere executar um teste com RDP.

### Aguardar a criação das impressoras

Use a política no Delivery Controller para habilitar o recurso no Citrix Virtual Desktops.

**Aguardar a criação de impressoras (Server Desktop):**

Essa configuração permite um atraso na conexão com uma sessão para que as impressoras redirecionadas do cliente possam ser criadas automaticamente.

Por padrão, um atraso de conexão não ocorre.

**Aguardar a criação de impressoras (Citrix Virtual Apps):**

A execução do seguinte cmdlet do PowerShell permite um atraso na conexão com aplicativos virtuais em execução em hosts de várias sessões para que as impressoras redirecionadas do cliente possam ser criadas automaticamente antes que o aplicativo seja aberto.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

Por padrão, um atraso de conexão não ocorre.

**Configurações de política de impressoras cliente**

A seção **Impressoras Cliente** inclui configurações de política para impressoras cliente, incluindo configurações para criar automaticamente impressoras cliente, reter propriedades da impressora e conectar-se a servidores de impressão.

#### CRIAR AUTOMATICAMENTE IMPRESSORAS CLIENTE

Esta configuração especifica as impressoras cliente que são criadas automaticamente. Esta configuração substitui as configurações padrão de criação automática de impressoras cliente.

Por padrão, todas as impressoras cliente são criadas automaticamente.

Esta configuração só entra em vigor se a configuração **Redirecionamento de impressora cliente** estiver presente e definida como **Permitido**.

Ao adicionar esta configuração a uma política, selecione uma opção:

- **Criar automaticamente todas as impressoras cliente** cria automaticamente todas as impressoras em um dispositivo de usuário.
- **Criar automaticamente apenas a impressora padrão do cliente** cria automaticamente apenas a impressora selecionada como impressora padrão no dispositivo do usuário.
- **Criar automaticamente apenas impressoras cliente locais (não de rede)** cria automaticamente apenas impressoras conectadas diretamente ao dispositivo do usuário através de uma porta LPT, COM, USB, TCP/IP ou outra porta local.

- **Não criar automaticamente impressoras cliente** desativa a criação automática para todas as impressoras cliente quando os usuários fazem logon. A escolha desta opção faz com que as configurações dos Serviços de Área de Trabalho Remota (RDS) para a criação automática de impressoras cliente substituam esta configuração em políticas de menor prioridade.

### CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL GENÉRICA

Esta configuração habilita ou desabilita a criação automática do objeto genérico Citrix Universal™ Printer para sessões. Essas sessões incluem apenas as sessões em que um dispositivo de usuário compatível com a Impressão Universal está em uso.

Por padrão, o objeto genérico Universal Printer não é criado automaticamente.

As seguintes configurações de política estão relacionadas:

- Uso do driver de impressão universal
- Preferência de driver universal

### CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL PDF

Essa configuração habilita ou desabilita a criação automática da impressora PDF Citrix para sessões usando:

- Citrix Workspace app para Windows (a partir do VDA 7.19)
- Citrix Workspace™ app para HTML5
- Aplicativo Citrix Workspace para Chrome

Por padrão, a impressora PDF Citrix não é criada automaticamente.

### NOMES DE IMPRESSORAS CLIENTE

Essa configuração seleciona a convenção de nomenclatura para impressoras cliente criadas automaticamente.

Por padrão, nomes de impressoras padrão são usados.

Selecione **Nomes de impressoras padrão** para usar nomes de impressoras como "HPLaserJet 4 do nome do cliente na sessão 3."

Selecione **Nomes de impressoras herdados** para usar nomes de impressoras cliente de estilo antigo e para preservar a compatibilidade com versões anteriores de nomes de impressoras herdados, como presentes nas versões XenDesktop do produto. Você pode usar essa opção com as versões atuais do produto Citrix Virtual Apps and Desktops. Um exemplo de nome de impressora herdado é "Client/clientname#/HPLaserJet 4." Essa opção é menos segura.

Ao usar a impressora PDF Citrix em uma sessão iniciada a partir do Citrix Workspace app para HTML5, defina a configuração **Nomes de impressoras cliente** como padrão ou selecione **Nomes de impressoras padrão**. Se você selecionar **Nomes de impressoras herdados**, o Citrix Workspace app para HTML5 não oferece suporte à opção Impressora PDF Citrix.

### CONEXÕES DIRETAS A SERVIDORES DE IMPRESSÃO

Essa configuração habilita ou desabilita conexões diretas do desktop virtual ou de aplicativos de hospedagem de servidor para um servidor de impressão para impressoras cliente. Aqui, as impressoras cliente são hospedadas em um compartilhamento de rede acessível.

Por padrão, as conexões diretas estão ativadas.

Ative as conexões diretas se o servidor de impressão em rede não estiver em uma WAN do desktop virtual ou dos aplicativos de hospedagem de servidor. A comunicação direta resulta em impressão mais rápida se o servidor de impressão em rede e o desktop virtual ou os aplicativos de hospedagem de servidor estiverem na mesma LAN.

Desative as conexões diretas se a rede estiver em uma WAN ou tiver latência substancial ou largura de banda limitada. Os trabalhos de impressão são roteados através do dispositivo do usuário, onde são redirecionados para o servidor de impressão em rede. Os dados enviados para o dispositivo do usuário são compactados, de modo que menos largura de banda é consumida à medida que os dados viajam pela WAN.

Se duas impressoras de rede tiverem o mesmo nome, a impressora na mesma rede que o dispositivo do usuário será usada.

### MAPEAMENTO E COMPATIBILIDADE DE DRIVER DE IMPRESSORA

Essa configuração especifica as regras de substituição de driver para impressoras cliente criadas automaticamente.

Essa configuração está definida para excluir o Microsoft OneNote e o XPS Document Writer da lista de impressoras cliente criadas automaticamente.

Ao definir regras de substituição de driver, você pode permitir ou impedir que impressoras sejam criadas com o driver especificado. Além disso, você pode permitir que as impressoras criadas usem apenas drivers de impressão universais. A substituição de driver substitui ou mapeia os nomes de driver de impressora fornecidos pelo dispositivo do usuário, substituindo um driver equivalente no servidor. Essas regras dão aos aplicativos de servidor acesso a impressoras cliente que têm os mesmos drivers que o servidor, mas nomes de driver diferentes.

Você pode fazer o seguinte:

- Adicionar um mapeamento de driver
- Editar um mapeamento existente
- Substituir configurações personalizadas para um mapeamento
- Remover um mapeamento
- Alterar a ordem das entradas de driver na lista

Ao adicionar um mapeamento, insira o nome do driver da impressora cliente e, em seguida, selecione o driver do servidor que você deseja substituir.

### RETENÇÃO DE PROPRIEDADES DA IMPRESSORA

Essa configuração especifica se as propriedades da impressora devem ser armazenadas e onde armazená-las.

Por padrão, o sistema determina se as propriedades da impressora são armazenadas no dispositivo do usuário, se disponível, ou no perfil do usuário.

Ao adicionar essa configuração a uma política, selecione uma opção:

- Salvo apenas no dispositivo cliente é para dispositivos de usuário que possuem um perfil obrigatório ou de roaming que não é salvo.
- Retido apenas no perfil do usuário é para dispositivos de usuário limitados pela largura de banda (esta opção reduz o tráfego de rede) e velocidade de logon ou para usuários com plug-ins legados. Esta opção armazena as propriedades da impressora no perfil do usuário no servidor e impede qualquer troca de propriedades com o dispositivo do usuário. Esta opção é aplicável apenas se um perfil de roaming do Remote Desktop Services (RDS) for usado.
- Mantido no perfil apenas se não salvo no cliente permite que o sistema determine onde as propriedades da impressora são armazenadas. As propriedades da impressora são armazenadas no dispositivo do usuário, se disponível, ou no perfil do usuário. Embora esta opção seja a mais flexível, ela também pode atrasar o tempo de logon e usar largura de banda extra para a verificação do sistema.
- Não reter propriedades da impressora impede o armazenamento de propriedades da impressora.

### IMPRESSORAS CLIENTE RETIDAS E RESTAURADAS

Esta configuração habilita ou desabilita a retenção e recriação de impressoras no dispositivo do usuário. Por padrão, as impressoras cliente são retidas e restauradas automaticamente.

Impressoras retidas são impressoras criadas pelo usuário que são criadas novamente, ou lembradas, no início da próxima sessão. Quando o Citrix Virtual Apps™ recria uma impressora retida, ele considera todas as configurações de política, exceto a configuração **Auto-create client printers**.

Impressoras restauradas são impressoras totalmente personalizadas por um administrador, com um estado salvo que está permanentemente anexado a uma porta cliente.

#### DRIVER DE IMPRESSORA UNIVERSAL PDF CITRIX

O driver de Impressora Universal PDF Citrix permite que os usuários imprimam documentos abertos com aplicativos hospedados ou aplicativos que estão sendo executados em desktops virtuais entregues pelo Citrix Virtual Apps and Desktops. Quando um usuário seleciona a opção **Citrix PDF Printer**, o driver converte o arquivo para PDF e transfere o PDF para o dispositivo local. O PDF é então aberto para visualização e impressão a partir de uma impressora conectada localmente. PDF é um dos formatos suportados com a Impressão Universal Citrix (além de EMF e XPS). A impressora PDF pode ser habilitada, configurada e definida como padrão usando uma Política Citrix. A opção **Citrix PDF Printer** está disponível para usuários do aplicativo Citrix Workspace para Windows, Chrome e HTML5.

> **Observação:**
>
> É necessário um visualizador de PDF para endpoints Windows. O cliente deve ter um aplicativo com associação de tipo de arquivo registrada no Windows para abrir arquivos PDF.

### Configurações de política de drivers

A seção **Drivers** inclui configurações de política relacionadas a drivers de impressora.

#### INSTALAÇÃO AUTOMÁTICA DE DRIVERS DE IMPRESSORA EMBUTIDOS

> **Observação**
>
> Esta política não oferece suporte a VDAs nesta versão.
>
> Esta configuração habilita ou desabilita a instalação automática de drivers de impressora a partir do seguinte:

- Conjunto de drivers embutidos do Windows
- Pacotes de drivers preparados no host usando `pnputil.exe /a`

Por padrão, esses drivers são instalados conforme necessário.

### PREFERÊNCIA DE DRIVER UNIVERSAL

Esta configuração especifica a ordem em que os drivers de impressora universais são usados, começando com a primeira entrada na lista.

Por padrão, a ordem de preferência é:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.

### USO DO DRIVER DE IMPRESSÃO UNIVERSAL

Esta configuração especifica quando usar a impressão universal.

Por padrão, a impressão universal é usada somente se o driver solicitado não estiver disponível.

A impressão universal emprega drivers de impressora genéricos em vez de drivers padrão específicos do modelo, simplificando potencialmente a carga de gerenciamento de drivers em computadores host. A disponibilidade de drivers de impressão universais depende dos recursos do dispositivo do usuário, do host e do software do servidor de impressão. Em certas configurações, a impressão universal pode não estar disponível.

Ao adicionar esta configuração a uma política, selecione uma opção na tabela a seguir:

| OPÇÃO | DESCRIÇÃO |
| --- | --- |
| **Usar apenas drivers específicos do modelo da impressora** | Especifica que a impressora cliente usa apenas os drivers padrão específicos do modelo que são criados automaticamente durante o logon. Se o driver solicitado não estiver disponível, a impressora cliente não poderá ser criada automaticamente. |

| OPÇÃO | DESCRIÇÃO |
| --- | --- |
| **Usar apenas impressão universal** | Especifica que nenhum driver padrão específico do modelo é usado. Apenas drivers de impressão universais são usados para criar impressoras. |
| **Usar impressão universal somente se o driver solicitado não estiver disponível** | Usa drivers padrão específicos do modelo para a criação da impressora, se estiverem disponíveis. Se o driver não estiver disponível no servidor, a impressora cliente será criada automaticamente com o driver universal apropriado. |
| **Usar drivers específicos do modelo da impressora somente se a impressão universal não estiver disponível** | Usa o driver de impressão universal se estiver disponível. Se o driver não estiver disponível no servidor, a impressora cliente será criada automaticamente com o driver de impressora específico do modelo apropriado. |

### Configurações de política do Universal Print Server

A seção **Universal Print Server** inclui configurações de política para lidar com o Universal Print Server.

#### CONJUNTO DE CIFRAS SSL

Essa configuração especifica o conjunto de conjuntos de cifras SSL/TLS que são usados no Universal Print Client para conexões de fluxo de dados de impressão criptografados (CGP).

Para controlar o pacote de conjuntos de cifras usado pelo Universal Print Client para conexões de serviço web de impressão criptografadas (HTTPS/SOAP), consulte .

Valor padrão: ALL

Essa configuração tem os seguintes valores: ALL, COM ou GOV.

Os conjuntos de cifras correspondentes a cada valor são os seguintes:

**ALL:**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

**COM:**

TLS_ECDHE_RSA_AES128_CBC_SHA

**GOV:**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

### MODO DE CONFORMIDADE SSL

Essa configuração especifica o nível de conformidade com a Publicação Especial NIST 800-52 que é usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão criptografados (CGP).

Valor padrão: Nenhum.

Essa configuração tem os seguintes valores:

**Nenhum.**

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade padrão.

**SP800-52.**

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade da Publicação Especial NIST 800-52.

### SSL ATIVADO

Essa configuração especifica se SSL/TLS é usado pelo Cliente de Impressão Universal para o seguinte:

- Conexões de fluxo de dados de impressão (CGP)
- Conexões de serviço web (HTTP/SOAP)

Quando você define **Ativar Universal Print Server** como **Ativado com fallback para impressão remota nativa do Windows**, as conexões de fallback são feitas pelo Provedor de Impressão de Rede do Microsoft Windows. Essa configuração não afeta essas conexões de fallback.

Valor padrão: Desabilitado

Esta configuração tem os seguintes valores:

**Habilitado.**

O Cliente de Impressão Universal usa SSL/TLS para se conectar ao Servidor de Impressão Universal.

**Desabilitado.**

O Universal Print Client usa SSL/TLS para se conectar ao Universal Print Server.

### MODO FIPS SSL

Esta configuração especifica se o módulo criptográfico SSL/TLS usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão (CGP) é executado no modo FIPS.

Valor padrão: Desabilitado

Esta configuração tem os seguintes valores:

**Habilitado.**

O modo FIPS está ativado.

**Desabilitado.**

O modo FIPS está desativado.

### VERSÃO DO PROTOCOLO SSL

Esta configuração especifica a versão do protocolo SSL/TLS usada pelo Cliente de Impressão Universal.

Valor padrão: ALL

Esta configuração tem os seguintes valores:

**ALL.**

Usar as versões TLS 1.0, 1.1 ou 1.2.

**TLSv1.**

Usar a versão TLS 1.0.

**TLSv1.1.**

Usar a versão TLS 1.1.

**TLSv1.2.**

Usar a versão TLS 1.2.

### PORTA SSL DO FLUXO DE DADOS DE IMPRESSÃO CRIPTOGRAFADOS (CGP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número da porta TCP da porta do fluxo de dados de impressão criptografados (CGP) do Universal Print Server. Esta porta recebe dados para trabalhos de impressão.

Valor padrão: 443

### PORTA SSL DO SERVIÇO WEB CRIPTOGRAFADO (HTTPS/SOAP) DO UNIVERSAL PRINT SERVER

Essa configuração especifica o número da porta TCP do serviço web criptografado (HTTPS/SOAP) do Universal Print Server. Essa porta recebe dados para comandos de impressão.

Valor padrão: 8443

### HABILITAR UNIVERSAL PRINT SERVER

Esta política habilita ou desabilita o uso do Citrix Universal Print Server (UPS). Aplique esta configuração de política a Unidades Organizacionais (OUs) que incluem o desktop virtual ou aplicativos de hospedagem de servidor. Esta configuração de política inclui opções de fallback para permitir conexões a servidores de impressão usando o serviço de impressão remota nativo do Windows, caso o componente Citrix UPS não esteja instalado ou indisponível no servidor de impressão solicitado. As alterações a esta política são aplicáveis somente após a reinicialização do VDA.

Por padrão, o Universal Print Server está desabilitado.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- **Habilitado com fallback para impressão remota nativa do Windows**: O Universal Print Server atende às conexões de impressora de rede, se possível. Se o Universal Print Server não estiver disponível, o Provedor de Impressão do Windows será usado. O Provedor de Impressão do Windows continua a manipular todas as impressoras criadas anteriormente com o Provedor de Impressão do Windows.
- **Habilitado sem fallback para impressão remota nativa do Windows**: O Universal Print Server atende exclusivamente às conexões de impressora de rede. Se o Universal Print Server estiver indisponível, a conexão da impressora de rede falhará. Essa configuração desabilita efetivamente a impressão em rede através do Provedor de Impressão do Windows.

As impressoras criadas anteriormente com o Provedor de Impressão do Windows não são criadas enquanto uma política contendo essa configuração estiver ativa.

- **Desabilitado**: O recurso Universal Print Server está desabilitado. Nenhuma tentativa é feita para conectar-se ao Universal Print Server ao conectar-se a uma impressora de rede com um nome UNC. As conexões com impressoras remotas continuam a usar o recurso de impressão remota nativo do Windows.

### PORTA DO FLUXO DE DADOS DE IMPRESSÃO (CGP) DO UNIVERSAL PRINT SERVER

Essa configuração especifica o número da porta TCP usada pelo listener do Common Gateway Protocol (CGP) do fluxo de dados de impressão do Universal Print Server. Aplique esta configuração de política apenas a OUs que contêm o servidor de impressão.

Por padrão, o número da porta é definido como 7229.

Os números de porta válidos devem estar no intervalo de 1 a 65535.

### LIMITE DE LARGURA DE BANDA DE ENTRADA DO FLUXO DE IMPRESSÃO DO UNIVERSAL PRINT SERVER (KBPS)

Essa configuração especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão. A taxa de transferência é calculada para os dados de impressão que são entregues de cada trabalho de impressão ao Universal Print Server usando CGP. Aplique esta configuração de política a OUs que contêm o desktop virtual ou aplicativos de hospedagem de servidor.

Por padrão, o valor é 0, o que especifica nenhum limite superior.

### PORTA DO SERVIÇO WEB (HTTP/SOAP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número da porta TCP usado pelo listener do serviço web (HTTP/SOAP) do Universal Print Server. O Universal Print Server é um componente opcional que permite o uso de drivers de impressão universais da Citrix para cenários de impressão em rede.

Quando o Universal Print Server é usado, os comandos de impressão são enviados dos hosts do Citrix Virtual Apps and Desktops para o Universal Print Server via SOAP sobre HTTP. Esta configuração modifica a porta TCP padrão na qual o Universal Print Server escuta as solicitações HTTP/SOAP de entrada.

Você deve configurar a porta HTTP do host e do servidor de impressão de forma idêntica. Se você não configurar as portas de forma idêntica, o software do host não se conectará ao Universal Print Server. Esta configuração altera o VDA no Citrix Virtual Apps and Desktops. Além disso, você deve alterar a porta padrão no Universal Print Server.

Por padrão, o número da porta é definido como 8080.

Os números de porta válidos devem estar no intervalo de 0 a 65535.

### UNIVERSAL PRINT SERVERS PARA BALANCEAMENTO DE CARGA

Esta configuração lista os Universal Print Servers a serem usados para balancear a carga das conexões de impressora estabelecidas no início da sessão, após avaliar outras configurações de política de impressão da Citrix®. Para otimizar o tempo de criação da impressora, a Citrix recomenda que todos os servidores de impressão tenham o mesmo conjunto de impressoras compartilhadas. Não há limite superior para o número de servidores de impressão que podem ser adicionados para balanceamento de carga.

Esta configuração também implementa a detecção de failover do servidor de impressão e a recuperação de conexões de impressora. Os servidores de impressão são verificados periodicamente quanto à disponibilidade. Se uma falha de servidor for detectada, esse servidor é removido do esquema de balanceamento de carga. Além disso, as conexões de impressora nesse servidor são redistribuídas entre outros servidores de impressão disponíveis. Quando o servidor de impressão com falha se recupera, ele é retornado ao esquema de balanceamento de carga.

Clique em **Validar Servidores** para verificar se cada servidor é um servidor de impressão, se a lista de servidores não inclui nomes de servidores duplicados e se todos os servidores têm um conjunto idêntico de impressoras compartilhadas instaladas. Esta operação pode levar algum tempo.

### LIMITE DE UNIVERSAL PRINT SERVERS FORA DE SERVIÇO

Esta configuração especifica quanto tempo o balanceador de carga deve esperar que um servidor de impressão indisponível se recupere antes de determinar que o servidor está permanentemente offline e redistribuir sua carga para outros servidores de impressão disponíveis.

Por padrão, o valor do limite é definido como 180 (segundos).

### TEMPO LIMITE DE CONEXÃO DO SERVIÇO WEB (HTTP/SOAP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número de segundos que o Cliente de Impressão Universal deve esperar até que uma operação connect() do serviço web do Servidor de Impressão Universal atinja o tempo limite. Esta configuração tem os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.

- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Cliente de Impressão Universal aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de socket TCP de conexão. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Cliente de Impressão Universal usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível nas versões anteriores do Cliente de Impressão Universal antes desta alteração.

O Cliente de Impressão Universal é o componente do Virtual Delivery Agent (VDA) que se comunica com o Servidor de Impressão Universal.

> **Nota:**
>
> Esta configuração de política é aplicável na versão 7.35 do VDA e posterior.

### TEMPO LIMITE DE RECEBIMENTO DO SERVIÇO WEB DO SERVIDOR DE IMPRESSÃO UNIVERSAL (HTTP/SOAP)

Esta configuração especifica o número de segundos que o Cliente de Impressão Universal deve esperar até que uma operação recv() do serviço web do Servidor de Impressão Universal atinja o tempo limite. Esta configuração tem os seguintes valores e todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Cliente de Impressão Universal aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de socket TCP de recebimento. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Cliente de Impressão Universal usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível nas versões anteriores do Cliente de Impressão Universal antes desta alteração.

O Universal Print Client é o componente do Virtual Delivery Agent (VDA) que se comunica com o Universal Print Server.

**Nota:**

Esta configuração de política é aplicável na versão 7.35 e posterior do VDA.

### TEMPO LIMITE DE ENVIO DO SERVIÇO WEB DO UNIVERSAL PRINT SERVER (HTTP/SOAP)

Esta configuração especifica o número de segundos que o Universal Print Client deve esperar até que uma operação send() do serviço web do Universal Print Server atinja o tempo limite. Esta configuração tem os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de envio de socket TCP. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível presente nas versões anteriores do Universal Print Client antes desta alteração.

O Universal Print Client é o componente do VDA que se comunica com o Universal Print Server.

**Nota:**

Esta configuração de política é aplicável na versão 7.35 e posterior do VDA.

### Configurações de política de impressão universal

A seção **Impressão Universal** inclui configurações de política para gerenciar a impressão universal.

### MODO DE PROCESSAMENTO EMF DE IMPRESSÃO UNIVERSAL

Esta configuração controla o método de processamento do arquivo de spool EMF no dispositivo de usuário Windows.

Por padrão, os registros EMF são enviados diretamente para a impressora.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Reprocessar EMFs para impressora força o arquivo de spool EMF a ser reprocessado e enviado através do subsistema GDI no dispositivo do usuário. Você pode usar esta configuração para drivers que exigem reprocessamento de EMF, mas que podem não ser selecionados automaticamente em uma sessão.
- Enviar diretamente para a impressora, quando usado com o driver de impressão Citrix Universal™, garante que os registros EMF sejam enviados e entregues ao dispositivo do usuário para processamento. Normalmente, esses arquivos de spool EMF são injetados diretamente na fila de spool do cliente. Para impressoras e drivers compatíveis com o formato EMF, este é o método de impressão mais rápido.

### LIMITE DE COMPRESSÃO DE IMAGEM DE IMPRESSÃO UNIVERSAL

Esta configuração especifica o seguinte:

- Qualidade máxima disponível para imagens impressas com o driver de impressão Citrix Universal
- Nível mínimo de compressão disponível para imagens impressas com o driver de impressão Citrix Universal

Por padrão, o limite de compactação de imagem é definido como Melhor qualidade (compactação sem perdas).

Se Nenhuma Compactação for selecionada, a compactação será desabilitada apenas para impressão EMF.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Sem compactação
- Melhor qualidade (compactação sem perdas)
- Alta qualidade
- Qualidade padrão
- Qualidade reduzida (compactação máxima)

Ao adicionar essa configuração a uma política que inclui a configuração **Padrões de otimização de impressão universal**, esteja ciente do seguinte:

- Considere que o nível de compactação na configuração **Limite de compactação de imagem de impressão universal** é menor do que o nível definido na configuração **Padrões de otimização de impressão universal**. Nesse caso, as imagens são compactadas no nível definido na configuração Limites de compactação de imagem de impressão universal.
- Se a compactação estiver desabilitada, as opções Qualidade de imagem desejada e Habilitar compactação pesada da configuração Padrões de otimização de impressão universal não terão efeito na política.

### PADRÕES DE OTIMIZAÇÃO DE IMPRESSÃO UNIVERSAL

Essa configuração especifica os valores padrão para otimização de impressão quando o driver de impressão universal é criado para uma sessão.

- A Qualidade de imagem desejada especifica o limite de compactação de imagem padrão aplicado à impressão universal. Por padrão, a Qualidade Padrão está habilitada, o que significa que os usuários só podem imprimir imagens usando compactação de qualidade padrão ou reduzida.
- Habilitar compactação pesada ativa ou desativa a redução da largura de banda além do nível de compactação definido pela Qualidade de imagem desejada, sem perda de qualidade da imagem. Por padrão, a compactação pesada está desabilitada.
- As configurações de Cache de imagem e fonte especificam se as imagens e fontes que aparecem várias vezes no fluxo de impressão devem ser armazenadas em cache ou não. Essa configuração garante que cada imagem ou fonte exclusiva seja enviada à impressora apenas uma vez. Por padrão, imagens e fontes incorporadas são armazenadas em cache. Essas configurações se aplicam somente se o dispositivo do usuário oferecer suporte a esse comportamento.
- Permitir que não administradores modifiquem essas configurações especifica se os usuários podem alterar as configurações padrão de otimização de impressão em uma sessão ou não. Por padrão, os usuários não têm permissão para alterar as configurações padrão de otimização de impressão.

Nota: Todas essas opções são suportadas para impressão EMF. Para impressão XPS, apenas a opção Qualidade de imagem desejada é suportada.

Ao adicionar esta configuração a uma política que inclui a configuração **Limite de compactação de imagem de impressão universal**, esteja ciente do seguinte:

- Considere que o nível de compactação na configuração **Limite de compactação de imagem de impressão universal** é menor do que o nível definido na configuração **Padrões de otimização de impressão universal**. Neste caso, as imagens são compactadas no nível definido na configuração Limites de compactação de imagem de impressão universal.
- Se a compactação estiver desabilitada, as opções Qualidade de imagem desejada e Habilitar compactação pesada da configuração Padrões de otimização de impressão universal não terão efeito na política.

### PREFERÊNCIA DE VISUALIZAÇÃO DE IMPRESSÃO UNIVERSAL

Esta configuração especifica se deve usar a função de visualização de impressão para impressoras universais genéricas ou criadas automaticamente.

Por padrão, a visualização de impressão não é usada para impressoras universais genéricas ou criadas automaticamente.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Não usar visualização de impressão para impressoras universais genéricas ou criadas automaticamente
- Usar visualização de impressão apenas para impressoras criadas automaticamente
- Usar visualização de impressão apenas para impressoras universais genéricas
- Usar visualização de impressão para impressoras universais genéricas e criadas automaticamente

### LIMITE DE QUALIDADE DE IMPRESSÃO UNIVERSAL

Esta configuração especifica o número máximo de pontos por polegada (dpi) disponível para gerar saída impressa em uma sessão.

Por padrão, Sem Limite está habilitado, o que significa que os usuários podem selecionar a qualidade máxima de impressão permitida pela impressora à qual se conectam.

Se esta configuração for configurada, ela limita a qualidade máxima de impressão disponível para os usuários em termos de resolução de saída. Tanto a própria qualidade de impressão quanto os recursos de qualidade de impressão da impressora à qual o usuário se conecta são restritos à configuração definida.

Por exemplo, se configurado para Resolução Média (600 DPI), os usuários podem imprimir a saída com uma qualidade máxima de 600 DPI apenas. Além disso, a configuração de **Qualidade**

**de Impressão** na guia **Avançado** da caixa de diálogo **Impressora Universal** mostra as configurações de resolução apenas até e incluindo Qualidade Média (600 DPI).

Ao adicionar esta configuração a uma política, selecione uma opção:

- Rascunho (150 DPI)
- Baixa Resolução (300 DPI)
- Média Resolução (600 DPI)
- Alta Resolução (1200 DPI)
- Sem Limite

## Configurações de política de segurança

A seção **Segurança** inclui a configuração de política para configurar a criptografia de sessão e a criptografia de dados de logon.

### Nível mínimo de criptografia SecureICA

Esta configuração especifica o nível mínimo no qual os dados da sessão enviados entre o servidor e um dispositivo de usuário devem ser criptografados.

**Importante:** Para o Virtual Delivery Agent 7.x, esta configuração de política pode ser usada apenas para habilitar a criptografia dos dados de logon com criptografia RC5 de 128 bits. Outras configurações são fornecidas apenas para compatibilidade retroativa com versões legadas do Citrix Virtual Apps and Desktops.

Para o VDA 7.x, a criptografia dos dados da sessão é definida usando as configurações básicas do Delivery Group do VDA. Se Habilitar Secure ICA for selecionado para o Delivery Group, os dados da sessão serão criptografados usando criptografia RC5 (128 bits). Se Habilitar Secure ICA não for selecionado para o Delivery Group, os dados da sessão serão criptografados com criptografia Básica.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Básico criptografa a conexão do cliente usando um algoritmo não-RC5. Ele protege o fluxo de dados de ser lido diretamente, mas pode ser descriptografado. Por padrão, o servidor usa criptografia Básica para o tráfego cliente-servidor.
- Logon RC5 (128 bits) criptografa apenas os dados de logon usando criptografia RC5 de 128 bits e a conexão do cliente usando criptografia Básica.
- RC5 (40 bits) criptografa a conexão do cliente usando criptografia RC5 de 40 bits.

- RC5 (56 bits) criptografa a conexão do cliente usando criptografia RC5 de 56 bits.
- RC5 (128 bits) criptografa a conexão do cliente usando criptografia RC5 de 128 bits.

As configurações que você especifica para a criptografia cliente-servidor podem interagir com quaisquer outras configurações de criptografia em seu ambiente e em seu sistema operacional Windows. Considere que um nível de criptografia de prioridade mais alta esteja definido em um servidor ou dispositivo de usuário. Nesse caso, as configurações que você especifica para recursos publicados podem ser substituídas.

Você pode aumentar os níveis de criptografia para proteger ainda mais as comunicações e a integridade das mensagens para determinados usuários. Se uma política exigir um nível de criptografia mais alto, os Citrix Receivers que usam um nível de criptografia mais baixo terão a conexão negada.

O SecureICA não realiza autenticação nem verifica a integridade dos dados. Para fornecer criptografia de ponta a ponta para seu site, use o SecureICA com criptografia TLS.

O SecureICA não usa algoritmos compatíveis com FIPS. Se essa configuração for um problema, configure o servidor e os Citrix Receivers para evitar o uso do SecureICA.

O SecureICA usa a cifra de bloco RC5, conforme descrito na RFC 2040, para confidencialidade. O tamanho do bloco é de 64 bits (um múltiplo de unidades de palavra de 32 bits). O comprimento da chave é de 128 bits. O número de rodadas é 12.

As chaves para a cifra de bloco RC5 são negociadas quando uma sessão é criada. A negociação é realizada usando o algoritmo Diffie-Hellman. Essa negociação usa parâmetros públicos Diffie-Hellman. Esses parâmetros são armazenados no registro do Windows quando o Virtual Delivery Agent é instalado. Os parâmetros públicos não são secretos. O resultado da negociação Diffie-Hellman é uma chave secreta, da qual as chaves de sessão para a cifra de bloco RC5 são derivadas. Chaves de sessão separadas são usadas para logon do usuário e para transferência de dados. Além disso, chaves de sessão separadas são usadas para o tráfego de e para o Virtual Delivery Agent. Portanto, há quatro chaves de sessão para cada sessão. As chaves secretas e as chaves de sessão não são armazenadas. Os vetores de inicialização para a cifra de bloco RC5 também são derivados da chave secreta.

### Configurações de política de limites de sessão

A seção **Limites de Sessão** inclui configurações de política que controlam por quanto tempo as sessões permanecem conectadas antes de serem forçadas a fazer logoff.

### Temporizador de sessão desconectada

Essa configuração habilita ou desabilita um temporizador que especifica por quanto tempo uma área de trabalho desconectada e bloqueada permanece bloqueada antes que a sessão seja desconectada.

Se este temporizador estiver habilitado, a sessão desconectada será desconectada quando o temporizador expirar.

Por padrão, as sessões desconectadas não são desconectadas.

### Temporizador de sessão desconectada do Acesso Remoto ao PC

Essa configuração habilita ou desabilita um temporizador que desconecta uma sessão de usuário desconectada após o temporizador expirar. Se você habilitar essa configuração, use a configuração **Intervalo do temporizador de sessão desconectada** para especificar quantos minutos uma área de trabalho desconectada permanece bloqueada antes que a sessão do usuário seja desconectada.

Por padrão, essa configuração está desabilitada.

### Intervalo do temporizador de sessão desconectada

Essa configuração especifica quantos minutos uma área de trabalho desconectada e bloqueada permanece bloqueada antes que a sessão seja desconectada.

Por padrão, o período de tempo é de 1.440 minutos (24 horas).

### Temporizador de sessão desconectada – Multi-sessão

Essa configuração habilita ou desabilita um temporizador para determinar por quanto tempo uma sessão RDS desconectada pode persistir antes que a sessão seja desconectada. Por padrão, este temporizador está desabilitado e as sessões desconectadas não são desconectadas.

### Intervalo do temporizador de sessão desconectada – Multi-sessão

Essa configuração determina quantos minutos uma sessão RDS desconectada pode persistir antes que a sessão seja encerrada. Por padrão, o período é de 1440 minutos (24 horas).

### Temporizador de conexão de sessão

Essa configuração habilita ou desabilita um temporizador que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop. Se esse temporizador estiver habilitado, a sessão será desconectada ou encerrada quando o temporizador expirar. A

configuração do Microsoft **Encerrar sessão quando os limites de tempo forem atingidos** determina o próximo estado da sessão.

Por padrão, esse temporizador está desabilitado.

**Intervalo do temporizador de conexão de sessão**

Essa configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e um desktop.

Por padrão, a duração máxima é de 1.440 minutos (24 horas).

**Temporizador de conexão de sessão – Multi-sessão**

Essa configuração habilita ou desabilita um temporizador que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um servidor de terminal. Por padrão, esse temporizador está desabilitado.

**Intervalo do temporizador de conexão de sessão – Multi-sessão**

Essa configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e uma sessão RDS. Por padrão, a duração máxima é de 1440 minutos (24 horas).

**Temporizador de inatividade da sessão**

Quando um usuário não fornece nenhuma entrada, essa configuração é usada para habilitar ou desabilitar:

- Um temporizador que especifica por quanto tempo uma conexão ininterrupta do dispositivo do usuário com um desktop é mantida.

Quando esse temporizador expira, a sessão é colocada no estado desconectado e o **Temporizador de sessão desconectada** é aplicado. Se o **Temporizador de sessão desconectada** estiver desabilitado, a sessão não será encerrada.

Por padrão, este temporizador está ativado.

**Intervalo do temporizador de inatividade da sessão**

Quando não há entrada do usuário, esta configuração é usada para especificar:

- O número de minutos durante os quais uma conexão ininterrupta de dispositivo de usuário a um desktop é mantida.

Por padrão, as conexões ociosas são mantidas por 1.440 minutos (24 horas).

### Temporizador de inatividade da sessão – Multi-sessão

Esta configuração ativa ou desativa um temporizador para determinar a duração máxima de uma conexão ociosa entre um dispositivo de usuário e um servidor de terminal. Por padrão, este temporizador está desativado.

### Intervalo do temporizador de inatividade da sessão – Multi-sessão

Esta configuração especifica quantos minutos uma conexão ociosa entre um dispositivo de usuário e uma sessão RDS. Por padrão, a duração máxima é de 1440 minutos (24 horas).

> **Nota:**

> As configurações de temporizador para máquinas multi-sessão configuradas usando políticas Citrix® devem substituir as configurações de temporizador configuradas através das Políticas de Grupo da Microsoft. Para evitar comportamento inesperado, recomendamos que você configure as configurações de temporizador usando um dos dois métodos.

## Configurações de política de confiabilidade da sessão

A seção de **confiabilidade da sessão** inclui configurações de política para gerenciar conexões de confiabilidade da sessão.

### Conexões de confiabilidade da sessão

Essa configuração permite ou impede que as sessões sejam mantidas abertas durante uma perda de conectividade de rede. A confiabilidade da sessão, juntamente com a reconexão automática do cliente, permite que os usuários se reconectem automaticamente às suas sessões do aplicativo Citrix Workspace™ após se recuperarem de interrupções de rede. Por padrão, a confiabilidade da sessão é Permitida.

As configurações no Web Studio são aplicadas no cliente para o seguinte:

- Aplicativo Citrix Workspace 1808 e posterior
- Citrix Receiver para Windows 4.7 e posterior.

A política do Web Studio substitui o Objeto de Política de Grupo do Citrix Receiver™ nos clientes. As atualizações dessas políticas no Web Studio sincronizam a confiabilidade da sessão do servidor para o cliente.

> **Observação:**

- Citrix Receiver para Windows 4.7 e posterior e aplicativos Citrix Workspace para Windows - Defina a política no Web Studio.
- Citrix Receivers para Windows anteriores a 4.7 - Defina as políticas no Web Studio. Defina também o modelo de Objeto de Política de Grupo do Citrix Receiver no cliente para um comportamento consistente.

A confiabilidade da sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Use a confiabilidade da sessão para manter a sessão ativa no servidor. Para indicar que a conectividade foi perdida, a exibição do usuário fica opaca. O usuário pode ver uma sessão congelada durante a interrupção. O usuário pode retomar a interação com o aplicativo quando a conexão de rede for restaurada. A confiabilidade da sessão reconecta os usuários sem prompts de reautenticação.

Se você usar a confiabilidade da sessão e a reconexão automática do cliente, os dois recursos funcionarão em sequência. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração de tempo limite de confiabilidade da sessão. Depois disso, as configurações de reconexão automática do cliente entram em vigor, tentando reconectar o usuário à sessão desconectada.

Por padrão, a confiabilidade da sessão é Permitida.

**Observação:**

Quando o Citrix ADC está em uso, você deve selecionar **Habilitar confiabilidade da sessão** no Citrix StoreFront > **Gerenciar Citrix Gateways** / **Secure Ticket Authority** para fazer proxy de conexões ICA.

### Número da porta de confiabilidade da sessão

Esta configuração especifica o número da porta TCP para conexões de confiabilidade da sessão de entrada.

Por padrão, o número da porta é definido como 2598.

#### Tempo limite de confiabilidade da sessão

Esta configuração especifica a duração, em segundos. Este tempo é o tempo que o proxy de confiabilidade da sessão aguarda um usuário para reconectar antes de permitir que a sessão seja desconectada.

Embora você possa estender o tempo em que uma sessão é mantida aberta, esse recurso é uma conveniência e não solicita ao usuário uma nova autenticação. Quanto mais tempo uma sessão fica aberta, maiores são as chances de um usuário deixar o dispositivo sem supervisão e potencialmente acessível a usuários não autorizados.

Por padrão, o tempo limite é definido como 180 segundos, ou três minutos.

### Configurações de política de marca d'água de sessão

A seção **marca d'água de sessão** inclui configurações de política para configurar este recurso. A habilitação deste recurso causa um aumento significativo na largura de banda da rede e no uso da CPU pela máquina VDA. Recomendamos que você configure a marca d'água de sessão para máquinas VDA selecionadas com base nos seus recursos de hardware disponíveis.

> **Importante**
>
> Habilite a marca d'água de sessão para que as outras configurações de política de marca d'água sejam eficazes. Para obter uma melhor experiência do usuário, não habilite mais de dois itens de texto de marca d'água.

#### Habilitar marca d'água da sessão

Quando você habilita esta configuração, a exibição da sessão tem uma marca d'água textual opaca exibindo informações específicas da sessão. As outras configurações de marca d'água dependem desta estar habilitada.

Por padrão, a marca d'água de sessão está desabilitada.

#### Incluir endereço IP do cliente

Quando você habilita esta configuração, a sessão exibe o endereço IP atual do cliente como uma marca d'água.

Por padrão, Incluir endereço IP do cliente está desabilitado.

### Incluir tempo de conexão

Quando você habilita esta configuração, a marca d'água da sessão exibe um tempo de conexão. O formato é aaaa/mm/dd hh:mm. A hora exibida é baseada no relógio do sistema e no fuso horário.

Por padrão, Incluir tempo de conexão está desabilitado.

### Incluir nome de usuário de logon

Quando você habilita esta configuração, a sessão exibe o nome de usuário de logon atual como uma marca d'água. O formato de exibição é USERNAME@DOMAINNAME. Recomendamos que o nome de usuário tenha no máximo 20 caracteres. Quando um nome de usuário tem mais de 20 caracteres, fontes de caracteres excessivamente pequenas ou truncamento podem ocorrer e diminuir a eficácia da marca d'água.

Por padrão, Incluir nome de usuário de logon está habilitado.

### Incluir nome do host VDA

Quando você habilita esta configuração, a sessão exibe o nome do host VDA da sessão ICA® atual como uma marca d'água.

Por padrão, Incluir nome do host VDA está habilitado.

### Incluir endereço IP do VDA

Quando você habilita esta configuração, a sessão exibe o endereço IP do VDA da sessão ICA atual como uma marca d'água.

Por padrão, o endereço IP do VDA está desativado.

### Estilo da marca d'água da sessão

Esta configuração controla se você exibe um único rótulo de texto de marca d'água ou vários rótulos. Escolha **Múltiplo** ou **Único** no menu suspenso **Valor**.

**Múltiplo** exibe cinco rótulos de marca d'água na sessão. Um no centro e quatro nos cantos.

**Único** exibe um único rótulo de marca d'água no centro da sessão.

Por padrão, o estilo da marca d'água da sessão é Múltiplo.

### Texto personalizado da marca d'água

Esta configuração permite aplicar texto personalizado (por exemplo, o nome da empresa) para exibir na marca d'água da sessão. Ao configurar uma string não vazia, ela exibe o texto em uma

nova linha, anexando outras informações ativadas na marca d'água. O texto personalizado da marca d'água é limitado a 25 caracteres Unicode. Se você configurar uma string mais longa, ela será truncada para 25 caracteres.

Não há texto padrão.

A partir do Citrix Virtual Apps and Desktops™ 7 2206, você pode adicionar mais personalização usando tags personalizadas no texto. Como resultado, o número máximo de caracteres no texto personalizado é aumentado para 1024.

As tags disponíveis para as configurações de marca d'água são descritas na tabela a seguir:

| TAG | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| `<font=value>` | Permite alterar a fonte do texto da marca d'água. O valor é o nome de uma fonte disponível no VDA. | `<font=Courier New>` |
| `<fontzoom=value>` | Permite definir a porcentagem do fator de zoom da fonte. O valor é 200 para zoom de 200% no texto da marca d'água. | `<fontzoom=200>` |
| `<position=value>` | Permite alterar a posição do texto da marca d'água. Os valores são `center`, `topleft`, `topright`, `bottomleft` e `bottomright`. Esta tag é aplicável apenas com estilo único. | `<position=topright>` |
| `<rotation=value>` | Permite girar o texto da marca d'água. O valor é especificado em graus e o intervalo é de -360 a 360. | `<rotation=45>` |
| `<style=value>` | Permite alterar o estilo de exibição. Esta tag substitui a política de estilo de marca d'água da sessão. | `<style=single>` |

Os seguintes estilos de marca d'água estão disponíveis:

- Estilo único - Um único rótulo de texto de marca d'água aparece no centro da sessão. Você pode usar a tag de posição para alterar o local.
- Estilo x ou múltiplo - Cinco rótulos de marca d'água aparecem na sessão - um no centro e um em cada canto.
- Lado a lado - Vários rótulos aparecem na sessão. O texto da marca d'água é colocado igualmente em toda a tela.

As tags disponíveis para alterar o texto da marca d'água são descritas na tabela a seguir:

| TAG | DESCRIÇÃO |
|---|---|
| `<clientip>` | O endereço IP do endpoint. |
| `<date>` | A data em que a sessão foi estabelecida. |
| `<domain>` | O nome de domínio da conta de usuário logada. |
| `<hostname>` | O nome da máquina do VDA. |
| `<newline>` | Cria uma linha extra. |
| `<serverip>` | O endereço IP do VDA. |
| `<time>` | A hora em que a sessão foi estabelecida. |
| `<username>` | O nome do usuário. |

**Nota:**

- A política **Texto personalizado da marca d'água** entra em vigor somente quando a política **Habilitar marca d'água da sessão** está habilitada. Seu valor padrão é *Desabilitado*.
- Se você usar as tags para alterar o texto da marca d'água, todas as outras políticas de marca d'água da sessão, exceto **Habilitar marca d'água da sessão**, serão ignoradas.

> Se você usar as tags para as configurações de texto da marca d'água, poderá usar todas as outras políticas de marca d'água.

#### Transparência da marca d'água

Você pode especificar a opacidade da marca d'água de 0 a 100. Quanto maior o valor especificado, mais opaca será a marca d'água.

Por padrão, o valor é 17.

### Configurações de política de controle de fuso horário

A seção **Controle de Fuso Horário** inclui configurações de política relacionadas ao uso da hora local nas sessões.

#### Estimar hora local para clientes legados

Essa configuração habilita ou desabilita a estimativa do fuso horário local dos dispositivos do usuário. Esses dispositivos incluem os dispositivos do usuário que enviam informações imprecisas de fuso horário para o servidor.

Por padrão, o servidor estima o fuso horário local quando necessário.

Essa configuração destina-se ao uso com Citrix Receivers legados ou clientes ICA que não enviam informações detalhadas de fuso horário para o servidor. Considere que essa configuração é usada com Citrix Receivers que enviam informações detalhadas de fuso horário para o servidor. Por exemplo, versões compatíveis do Citrix Receiver™ para Windows. Nesse caso, essa configuração não tem efeito.

#### Restaurar fuso horário do SO da área de trabalho na desconexão ou logoff da sessão

Considere que o usuário se desconecta ou faz logoff de uma sessão. Nesse caso, essa configuração determina se a configuração de fuso horário para um VDA de SO de sessão única é restaurada para o fuso horário original da máquina. Se você habilitar essa configuração, o VDA restaurará o fuso horário da máquina para sua configuração original quando o usuário se desconectar ou fizer logoff. Para que essa configuração tenha efeito, defina **Usar hora local do cliente** como **Usar fuso horário do cliente**.

Por padrão, essa configuração está habilitada.

### Usar hora local do cliente

Essa configuração determina a configuração de fuso horário da sessão do usuário. As opções são o fuso horário da sessão do usuário (fuso horário do servidor) ou o fuso horário do dispositivo do usuário (fuso horário do cliente).

Por padrão, o fuso horário da sessão do usuário é usado.

Para que essa configuração tenha efeito, habilite a configuração **Permitir redirecionamento de fuso horário** no Editor de Política de Grupo. A configuração está em **Política de Computador Local** > **Configuração do Computador** > **Modelos Administrativos** > **Componentes do Windows** > **Serviços de Área de Trabalho Remota** > **Host da Sessão da Área de Trabalho Remota** > **Redirecionamento de Dispositivos e Recursos**.

Se você estiver usando VDA de sessão única (anteriormente conhecido como VDA de Estação de Trabalho) em máquinas que executam um SO de servidor, configure o direito de usuário local **Alterar o fuso horário** para **Todos**. Esse direito de usuário pode ser encontrado em **Política de Computador Local** > **Configuração do Computador** > **Configurações do Windows** > **Configurações de Segurança** > **Políticas Locais** > **Atribuição de Direitos de Usuário**.

> **Nota:**
>
> Em um SO de sessão única, os **Usuários** estão incluídos na Atribuição de Direitos de Usuário **Alterar o fuso horário**, embora não em um SO de várias sessões. Em um SO de várias sessões, o fuso horário é sincronizado usando a seguinte política de grupo: Configuração do Computador\Modelos Administrativos\Componentes do Windows\Serviços de Área de Trabalho Remota\Host da Sessão da Área de Trabalho Remota\Redirecionamento de Dispositivos e Recursos\Permitir redirecionamento de fuso horário. Essa política é aplicável quando o Servidor é um Host da Sessão da Área de Trabalho Remota no VDA de SO de várias sessões (instalado com o comando `/ServerVDI`). Em um SO de várias sessões, por padrão e por design, os usuários não têm o direito local de alterar o fuso horário.

## Configurações de política de dispositivos TWAIN

A seção **Dispositivos TWAIN** inclui configurações de política relacionadas ao seguinte:

- Mapeamento de dispositivos TWAIN do cliente, como câmeras digitais ou scanners
- Otimização de transferências de imagem do servidor para o cliente

> **Observação:**
>
> O TWAIN 2.0 é compatível com o Citrix Receiver para Windows 4.5.

#### Redirecionamento de dispositivo TWAIN do cliente

Os dispositivos TWAIN se comunicam com aplicativos de processamento de imagem hospedados no servidor usando o protocolo TWAIN.

Essa configuração permite ou impede que os usuários acessem dispositivos TWAIN no dispositivo do usuário. Por padrão, o redirecionamento de dispositivo TWAIN é permitido.

As seguintes configurações de política estão relacionadas:

- Nível de compactação TWAIN
- Limite de largura de banda de redirecionamento de dispositivo TWAIN
- Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN

#### Nível de compactação TWAIN

Essa configuração especifica o nível de compactação das transferências de imagem do cliente para o servidor. Use Baixo para melhor qualidade de imagem, Médio para boa qualidade de imagem ou Alto para baixa qualidade de imagem. Por padrão, a compactação média é aplicada.

### Configurações de política de dispositivos USB

A seção **Dispositivos USB** inclui configurações de política para gerenciar o redirecionamento de arquivos para dispositivos USB.

#### Regras de otimização de dispositivos USB do cliente

As regras de otimização de dispositivos USB do cliente podem ser aplicadas a dispositivos para desabilitar a otimização ou para alterar o modo de otimização.

Quando um usuário conecta um dispositivo de entrada USB, o host verifica se as configurações da **política USB** permitem o dispositivo. Se o dispositivo for permitido, o host verifica as **regras de otimização de dispositivos USB do cliente** para o dispositivo. Se nenhuma regra for especificada, o dispositivo não será otimizado. O modo de captura (04) é o modo recomendado para dispositivos de assinatura. Para outros dispositivos que apresentam desempenho degradado em latências mais altas, os administradores podem habilitar o modo interativo (02). Consulte as descrições dos modos disponíveis na tabela neste artigo.

### É bom saber

- Para o uso de mesas digitalizadoras e tablets Wacom, recomendamos que você desative o protetor de tela. As etapas sobre como desativar o protetor de tela estão no final desta seção.
- O suporte para a otimização de mesas digitalizadoras e tablets da série Wacom STU foi pré-configurado na instalação das políticas do Citrix Virtual Apps and Desktops™.
- Os dispositivos de assinatura funcionam em todo o Citrix Virtual Apps and Desktops e não exigem um driver para serem usados como um dispositivo de assinatura. A Wacom possui mais software que pode ser instalado para personalizar ainda mais o dispositivo. Consulte `<http://www.wacom.com/>`.
- Tablets de desenho. Certos dispositivos de entrada de desenho podem se apresentar como um dispositivo HID em barramentos PCI/ACPI e não são suportados. Conecte esses dispositivos a um controlador de host USB no cliente para serem redirecionados dentro de uma sessão do Citrix Virtual Desktops.

As regras de política seguem o formato de expressões tag=valor separadas por espaço em branco. As seguintes tags são suportadas:

| NOME DA TAG | DESCRIÇÃO |
|---|---|
| Modo | O modo de otimização é suportado para dispositivos de entrada para class=**03**. Os modos suportados são: Sem otimização - valor **01**. Modo interativo - valor **02**. Recomendado para dispositivos como tablets de caneta e mouses 3D Pro. Modo de captura - valor **04**. Preferencial para dispositivos como mesas de assinatura. |
| VID | ID do Fornecedor do descritor do dispositivo, como um número hexadecimal de quatro dígitos. |
| PID | ID do produto do descritor do dispositivo, como um número hexadecimal de quatro dígitos. |
| REV | ID de revisão do descritor do dispositivo, como um número hexadecimal de quatro dígitos. |
| Classe | Classe do descritor do dispositivo ou de um descritor de interface. |

| NOME DA TAG | DESCRIÇÃO |
| --- | --- |
| Subclasse | Subclasse do descritor do dispositivo ou de um descritor de interface. |
| Prot | Protocolo do descritor do dispositivo ou de um descritor de interface. |

**Exemplos**

Mode=00000004 VID=067B PID=1230 class=03 #Dispositivo de entrada operando no modo de captura

Mode=00000002 VID=067B PID=1230 class=03 #Dispositivo de entrada operando no modo interativo (padrão)

Mode=00000001 VID=067B PID=1230 class=03 #Dispositivo de entrada operando sem qualquer otimização

Mode=00000100 VID=067B PID=1230 # Otimização de configuração do dispositivo desabilitada (padrão)

Mode=00000200 VID=067B PID=1230 # Otimização de configuração do dispositivo habilitada

**Desativando o protetor de tela para dispositivos de assinatura Wacom**

Para o uso de pads e tablets de assinatura Wacom, a Citrix® recomenda que você desative o protetor de tela da seguinte forma:

1. Instale o **Wacom-STU-Driver** após redirecionar o dispositivo.
2. Instale o **Wacom-STU-Display MSI** para ter acesso ao painel de controle da mesa digitalizadora.
3. Vá para **Painel de Controle > Wacom STU Display > STU430** ou **STU530** e selecione a guia do seu modelo.
4. Escolha **Alterar** e, em seguida, selecione **Sim** quando a janela de segurança do UAC aparecer.
5. Selecione **Desativar apresentação de slides** e, em seguida, **Aplicar**.

Depois que a configuração é definida para um modelo de mesa digitalizadora, ela é aplicada a todos os modelos.

### Redirecionamento de dispositivo USB do cliente

Esta configuração permite ou impede o redirecionamento de dispositivos USB para e do dispositivo do usuário.

Por padrão, os dispositivos USB não são redirecionados.

### Regras de redirecionamento de dispositivo USB do cliente

Esta configuração especifica as regras de redirecionamento para dispositivos USB.

Por padrão, nenhuma regra é especificada.

Quando um usuário conecta um dispositivo USB, o dispositivo host o verifica em relação a cada regra de política, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva. Se a primeira correspondência for uma regra de Permissão, o dispositivo é redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo estará disponível apenas para o desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

As regras da política seguem o formato {Allow:|Deny:} seguido por um conjunto de expressões tag=valor separadas por espaços em branco. As seguintes tags são suportadas:

| NOME DA TAG | DESCRIÇÃO |
|---|---|
| VID | ID do Fornecedor do descritor do dispositivo |
| PID | ID do Produto do descritor do dispositivo |
| REL | ID de Lançamento do descritor do dispositivo |
| Classe | Classe do descritor do dispositivo ou de um descritor de interface |
| Subclasse | Subclasse do descritor do dispositivo ou de um descritor de interface |
| Prot | Protocolo do descritor do dispositivo ou de um descritor de interface |

Ao criar regras de política, lembre-se:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por #.

- Linhas em branco e linhas de comentário puro são ignoradas.
- As tags devem usar o operador de correspondência = (por exemplo, VID=067B_.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.
- Consulte os códigos de classe USB disponíveis no site do USB Implementers Forum, Inc.

Exemplos de regras de política USB definidas pelo administrador:

- Permitir: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Negar: Class=08 subclass=05 # Armazenamento em Massa
- Para criar uma regra que nega todos os dispositivos USB, use "DENY:" sem outras tags.

**Redirecionamento de dispositivo USB plug and play do cliente**

Essa configuração permite ou impede que dispositivos plug-and-play, como câmeras ou dispositivos de ponto de venda (POS), sejam usados em uma sessão de cliente.

Por padrão, o redirecionamento de dispositivos plug-and-play é permitido. Quando definido como Permitido, todos os dispositivos plug-and-play para um usuário ou grupo específico são redirecionados. Quando definido como Proibido, nenhum dispositivo é redirecionado.

**Configurar o redirecionamento automático de dispositivos USB**

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB.

> **Nota:**
>
> No Receiver para Windows 4.2, os dispositivos USB também são redirecionados automaticamente ao operar no modo de Dispositivo de Área de Trabalho. Além disso, a barra de conexão não está presente. Em versões anteriores do Citrix Receiver para Windows, os dispositivos USB também são redirecionados automaticamente ao operar no seguinte:
>
> - Modo de dispositivo de área de trabalho
> - Aplicativos hospedados em máquina virtual (VM)

> Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que dispositivos USB sejam listados ou redirecionados, use DeviceRules no endpoint do cliente ou na política DDC. Consulte os Guias de Administração para obter mais detalhes.

> **Cuidado:**

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

### CONFIGURAÇÕES DE PREFERÊNCIAS DO USUÁRIO PARA REDIRECIONAMENTO AUTOMÁTICO DE DISPOSITIVOS USB

Política:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
2. Abra **Novos Dispositivos USB**, selecione **Ativado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Ativado** e clique em **OK**.

Citrix Receiver:

1. Vá para **Preferências do Citrix Receiver > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
   - Quando uma sessão é iniciada, conectar dispositivos automaticamente
   - Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

Todas as chaves de registro e as alterações de política são aplicadas ao dispositivo cliente Windows.

### REDIRECIONAMENTO DE IMPRESSORAS USB SIMPLES

A melhor solução para impressoras USB simples é usar o Driver de Impressora Universal dedicado e o canal virtual para realizar a impressão. Por padrão, as impressoras USB simples não são redirecionadas automaticamente.

As impressoras simples são detectadas usando heurísticas. Além disso, espera-se que impressoras avançadas com funções de digitalização, por exemplo, possam precisar ser redirecionadas usando o suporte USB para funcionar completamente.

Use este registro para configurar se as impressoras simples são redirecionadas automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Tipo: DWORD

Dados: 00000000

O valor padrão é 0 (não redireciona automaticamente). Alterar o valor para qualquer número maior que zero habilita o suporte USB para redirecionar impressoras USB simples.

Você também pode implantar políticas do Active Directory para esta chave de registro e substituir o valor não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

### REDIRECIONAMENTO DE DISPOSITIVOS DE ÁUDIO SIMPLES

Assim como as impressoras simples, a melhor experiência do usuário é obtida usando o canal virtual de áudio dedicado do ICA® para enviar dados de áudio de dispositivos de áudio simples. No entanto, pode ser necessário redirecionar alguns dispositivos especiais usando o suporte USB. Heurísticas são usadas para determinar quais dispositivos são dispositivos de áudio simples.

Use este registro no endpoint do cliente para configurar se os dispositivos de áudio simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para um número diferente de zero redireciona dispositivos de áudio USB simples com suporte USB.

Você pode usar políticas do Active Directory para implantar este valor na chave de registro e substituir o valor não-político se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectVideo

Tipo: DWORD

Dados: 00000000

### REDIRECIONAMENTO DE DISPOSITIVOS DE ARMAZENAMENTO SIMPLES (DISPOSITIVO DE ARMAZENAMENTO EM MASSA)

Para dispositivos de armazenamento simples, você obtém a melhor experiência do usuário usando o canal virtual dedicado, como o mapeamento de unidade cliente que também realiza otimização. Além da leitura ou gravação simples de arquivos, para executar certas tarefas especiais como gravar um CD/DVD ou acessar dispositivos de sistemas de arquivos criptografados, o dispositivo ainda pode precisar ser redirecionado usando o suporte USB genérico.

Heurísticas são usadas para determinar quais dispositivos são dispositivos de armazenamento simples. Use esta chave de registro para configurar se os dispositivos de armazenamento simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos de armazenamento USB simples usando suporte USB genérico.

Você também pode usar políticas do Active Directory para implantar este valor na seguinte chave de registro e substituir o valor não-político se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

> **Nota:**
>
> O acesso somente leitura ao dispositivo de armazenamento simples não é configurável se você estiver usando o suporte USB genérico, enquanto é configurável se estiver usando o CDM.

### REDIRECIONAMENTO DE UNIDADES FLASH USB COM CRIPTOGRAFIA DE HARDWARE

Unidades flash USB com criptografia de hardware geralmente consistem em uma partição de armazenamento criptografada e uma segunda partição de *utilitário* que contém um utilitário para desbloquear a partição criptografada. Para dispositivos de unidade flash USB, obtenha a melhor experiência do usuário usando o canal virtual HDX dedicado de mapeamento de unidade cliente/ mapeamento de unidade removível dinâmica que também realiza otimização.

O redirecionamento USB genérico é necessário para o seguinte:

- Clientes não-Windows (por exemplo, clientes Linux)
- Clientes onde o cliente restringiu (bloqueou) o acesso do usuário a funções locais no cliente

O redirecionamento USB genérico pode redirecionar qualquer dispositivo de armazenamento USB sem criptografia de hardware para sessões VDA de SO de sessão única e SO de múltiplas sessões.

Antes do Citrix Virtual Apps and Desktops 7 1808, unidades flash USB com criptografia de hardware não podiam ser redirecionadas de forma útil para sessões VDA de SO de sessão única ou SO de múltiplas sessões. Uma nova melhoria de recurso introduzida no Citrix Virtual Apps and Desktops 7 1808 suporta o redirecionamento USB genérico de unidades flash USB com criptografia de hardware para sessões VDA de SO de sessão única e SO de múltiplas sessões. Após o redirecionamento do dispositivo, nenhuma de suas unidades aparece no cliente local.

Portanto, se o desbloqueio da unidade for necessário, execute-o na sessão. Este recurso requer a atualização do Windows KB4074590.

### DISPOSITIVOS DE IMAGEM ESTÁTICA SIMPLES (SCANNERS E CÂMERAS DIGITAIS)

Para dispositivos de imagem estática simples, obtenha a melhor experiência do usuário usando o canal virtual dedicado (como o canal virtual TWAIN) que também realiza otimização. Esses dispositivos devem aderir aos padrões da indústria. Considere que um dispositivo não está em conformidade ou não é usado de acordo com as intenções originais. Neste caso, o redirecionamento USB genérico pode ser a única maneira de usar o dispositivo. Heurísticas são usadas para determinar quais dispositivos são dispositivos de imagem estática simples.

Use esta chave de registro para configurar se dispositivos de imagem estática simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos de imagem estática USB simples com USB genérico.

Você também pode usar políticas do Active Directory para implantar esse valor nesta chave de registro e substituir o valor não-política, se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dados: 00000000

### CONFIGURAÇÕES ESPECÍFICAS DO DISPOSITIVO

As heurísticas usadas para selecionar dispositivos otimizáveis Citrix nem sempre correspondem ao que você deseja. Os exemplos de dispositivos otimizáveis Citrix são impressoras, áudio, vídeo, armazenamento e dispositivos de imagem estática. Você pode querer controlar o redirecionamento automático de dispositivos que não estão listados acima. Você pode controlar o redirecionamento automático com base em cada dispositivo.

Por exemplo, o leitor de código de barras DemoTech 2.000 não precisa ser redirecionado usando o suporte USB. Ele tem um identificador de fornecedor de 12AB e um identificador de produto de 5678. Esses números hexadecimais podem ser encontrados no Gerenciador de Dispositivos.

Para evitar que isso seja redirecionado automaticamente, crie esta chave de registro específica do dispositivo:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dados: 00000000

Um valor de 0 impede que o dispositivo seja redirecionado automaticamente. Um valor diferente de zero indica que o dispositivo deve ser considerado para redirecionamento automático (sujeito às preferências do usuário). Há um único caractere de espaço entre os identificadores de fornecedor e produto.

Você também pode implantar esse valor usando políticas do Active Directory para esta chave de registro. Ele substitui o valor não-político se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dados: 00000000

As configurações de AutoRedirect específicas do dispositivo têm precedência sobre os valores AutoRedirectXXX mais gerais explicados acima. As heurísticas padrão para dispositivos otimizados da Citrix podem interpretar erroneamente um dispositivo como genérico. Portanto, defina o valor AutoRedirect específico do dispositivo como 1 para redirecioná-lo automaticamente.

**Permitir que dispositivos USB existentes sejam conectados automaticamente**

Essa configuração permite ou impede a conexão automática dos dispositivos USB existentes que estão conectados ao endpoint no início de uma sessão à sessão remota.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- Perguntar antes de redirecionar dispositivos USB disponíveis.

- Não redirecionar automaticamente dispositivos USB disponíveis.
- Redirecionar automaticamente os dispositivos USB disponíveis.

Por padrão, a opção **Perguntar antes de redirecionar dispositivos USB disponíveis** é selecionada. Com base na política selecionada, a opção selecionada na seção **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Observação:**
>
> Atualmente, a política **Permitir que dispositivos USB existentes sejam conectados automaticamente** é aplicável apenas para o aplicativo Citrix Workspace™ para Windows.

**Permitir que dispositivos USB recém-conectados sejam automaticamente conectados**

Essa configuração permite ou impede a conexão automática dos dispositivos USB que são inseridos no endpoint durante uma sessão para a sessão remota.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- Perguntar antes de redirecionar dispositivos USB disponíveis.
- Não redirecionar automaticamente os dispositivos USB disponíveis.
- Redirecionar automaticamente os dispositivos USB disponíveis.

Por padrão, a opção **Perguntar antes de redirecionar dispositivos USB disponíveis** é selecionada. Com base na política selecionada, a opção selecionada na seção **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Observação:**
>
> Atualmente, a política **Permitir que dispositivos USB recém-conectados sejam automaticamente conectados** é aplicável apenas para o aplicativo Citrix Workspace para Windows.

**Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**

Essa configuração especifica regras para filtrar, dividir e conectar automaticamente dispositivos USB a uma sessão remota.

Quando esta configuração é selecionada, o host substitui a configuração *Regras de redirecionamento de dispositivo USB do cliente* pelas regras de dispositivo configuradas nesta configuração.

Para obter mais informações, consulte Configurando o redirecionamento de dispositivo USB composto.

### Configurações de política de lista de permissões de canal virtual

A configuração de política **Lista de permissões de canal virtual** permite o uso de uma lista de permissões que especifica quais canais virtuais podem ser abertos em uma sessão ICA®.

Quando desativado, todos os canais virtuais são permitidos.

Quando ativado, apenas os canais virtuais Citrix® são permitidos.

Para usar canais virtuais personalizados ou de terceiros, adicione os canais virtuais à lista. Para adicionar um canal virtual à lista:

1. Insira o nome do canal virtual seguido por uma vírgula.
2. Insira o caminho para o processo que acessa o canal virtual.

Mais caminhos executáveis podem ser listados, e os caminhos são separados por vírgulas.

Por exemplo,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

A partir do Citrix Virtual Apps and Desktops 7 2109, as listas de permissões de canal virtual são ativadas por padrão. Para obter mais informações sobre como adicionar canais virtuais à lista de permissões, consulte Adicionar canais virtuais à lista de permissões

Se você estiver usando o HDX RealTime Optimization Pack para Skype for Business, adicione o canal virtual à lista de permissões. Para obter mais informações, consulte a documentação do HDX RealTime Optimization Pack.

> **Importante:**
>
> As máquinas VDA devem ser reiniciadas para que a configuração entre em vigor.

> Para obter mais informações sobre canais virtuais, consulte canais virtuais ICA.

#### Registro da lista de permissões de canal virtual

Você pode usar esta configuração de política para configurar o nível de registro da Lista de Permissões de Canal Virtual.

As seguintes opções estão disponíveis:

| Opções | Descrição |
|---|---|
| Desativado | Desativa todos os eventos de log. |
| Registrar apenas avisos | Os eventos são registrados apenas para Canais Virtuais personalizados que tentam abrir e que não fazem parte da lista de permissões. |
| Registrar todos os eventos | Todos os eventos são registrados |

#### Limitação de log da lista de permissões de canais virtuais

Você pode usar essa configuração de política para configurar a frequência de registro de eventos para uma sessão ativa.

Todos os eventos para cada canal virtual serão registrados em sua primeira ocorrência. Eventos repetidos serão suprimidos durante o período de limitação enquanto a sessão estiver ativa. Se uma sessão for desconectada, o período de limitação será redefinido.

### Configurações de política de exibição visual

A seção **Exibição Visual** inclui configurações de política para controlar a qualidade das imagens que são enviadas de desktops virtuais para o dispositivo do usuário.

#### Profundidade de cor preferida para gráficos simples

Essa configuração de política está disponível nas versões 7.6 FP3 e posteriores do VDA. A opção de 8 bits está disponível nas versões 7.12 e posteriores do VDA.

Essa configuração possibilita diminuir a profundidade de cor na qual gráficos simples são enviados pela rede. A redução para 8 bits ou 16 bits por pixel pode melhorar a capacidade de resposta em conexões de baixa largura de banda. No entanto, essa ação pode causar uma leve degradação na qualidade da imagem. A profundidade de cor de 8 bits não é suportada quando a

configuração de política Usar codec de vídeo para compactação está definida como **Para a tela inteira**.

A profundidade de cor preferida padrão é de 24 bits por pixel.

Os VDAs voltam para a profundidade de cor de 24 bits (padrão) se a configuração de 8 bits for aplicada na versão 7.11 e anteriores do VDA.

**Taxa de quadros alvo**

Esta configuração especifica o número máximo de quadros por segundo enviados do desktop virtual para o dispositivo do usuário.

Por padrão, o máximo é de 30 quadros por segundo.

Definir um alto número de quadros por segundo (por exemplo, 30) melhora a experiência do usuário, mas requer mais largura de banda. Diminuir o número de quadros por segundo (por exemplo, 10) maximiza a escalabilidade do servidor em detrimento da experiência do usuário. Para dispositivos de usuário com CPUs mais lentas, especifique um valor menor para melhorar a experiência do usuário.

A taxa de quadros máxima suportada por segundo é 60.

**Qualidade visual**

Esta configuração especifica a qualidade visual desejada para as imagens exibidas no dispositivo do usuário.

Por padrão, essa configuração é Média.

Para especificar a qualidade das imagens, escolha uma das seguintes opções:

- **Baixa** - Recomendado para redes com largura de banda limitada, onde a qualidade visual pode ser sacrificada em prol da interatividade
- **Média** - Oferece o melhor desempenho e eficiência de largura de banda na maioria dos casos de uso
- **Alta** - Recomendado se você precisar de qualidade de imagem visualmente sem perdas
- **Construir para sem perdas** - Envia imagens com perdas para o dispositivo do usuário durante períodos de alta atividade de rede e imagens sem perdas após a redução da atividade de rede. Essa configuração melhora o desempenho em conexões de rede com largura de banda limitada

- **Sempre sem perdas** - Quando a preservação dos dados da imagem é vital, selecione **Sempre sem perdas** para garantir que dados com perdas nunca sejam enviados para o dispositivo do usuário. Por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável.

### Configurações de política de imagens em movimento

A seção **Imagens em Movimento** contém configurações que permitem remover ou alterar a compactação para imagens dinâmicas.

#### QUALIDADE MÍNIMA DA IMAGEM

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Legacy graphics mode está ativada.

Esta configuração especifica a qualidade mínima aceitável da imagem para o Adaptive Display. Quanto menos compactação for usada, maior será a qualidade das imagens exibidas. Escolha entre compactação Ultra Alta, Muito Alta, Alta, Normal ou Baixa.

Por padrão, isso é definido como Normal.

#### COMPACTAÇÃO DE IMAGEM EM MOVIMENTO

Esta configuração especifica se o Adaptive Display está ativado ou não. O Adaptive Display ajusta automaticamente a qualidade da imagem de vídeos e slides de transição em apresentações com base na largura de banda disponível. Com o Adaptive Display ativado, os usuários devem ver apresentações fluidas sem redução na qualidade.

Por padrão, o Adaptive Display está ativado.

Para as versões 7.0 a 7.6 do VDA, esta configuração se aplica somente quando o Legacy graphics mode está ativado. Para as versões 7.6 FP1 e posteriores do VDA, esta configuração se aplica quando o Legacy graphics mode está ativado, ou quando o Legacy graphics mode está desativado e um codec de vídeo não é usado para compactar gráficos.

Quando o Legacy graphics mode está ativado, a sessão deve ser reiniciada antes que as alterações de política entrem em vigor. O Adaptive Display é mutuamente exclusivo com o Progressive Display; ativar o Adaptive Display desativa o Progressive Display e vice-versa. No entanto, tanto o Progressive Display quanto o Adaptive Display podem ser desativados ao mesmo tempo. O Progressive Display, como um recurso herdado, não é recomendado para XenApp ou XenDesktop. Definir o Progressive threshold Level desativará o Adaptive Display.

### NÍVEL DE COMPRESSÃO PROGRESSIVA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Legacy graphics mode está ativada.

Esta configuração oferece uma exibição inicial de imagens menos detalhada, mas mais rápida.

Por padrão, nenhuma compactação progressiva é aplicada.

A imagem mais detalhada, definida pela configuração de compactação com perdas normal, aparece quando disponível. Use compactação Muito Alta ou Ultra Alta para uma visualização aprimorada de gráficos que consomem muita largura de banda, como fotografias.

Para que a compressão progressiva seja eficaz, seu nível de compressão deve ser maior do que a configuração de nível de compressão com perdas.

Nota: O nível aumentado de compressão associado à compressão progressiva também melhora a interatividade de imagens dinâmicas em conexões de cliente. A qualidade de uma imagem dinâmica, como um modelo tridimensional rotativo, é temporariamente diminuída até que a imagem pare de se mover, momento em que a configuração normal de compressão com perdas é aplicada.

As seguintes configurações de política estão relacionadas:

- Valor limite de compressão progressiva
- Compressão progressiva pesada

### VALOR LIMITE DE COMPRESSÃO PROGRESSIVA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está ativada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual a compressão progressiva é aplicada. Isso é aplicado apenas a conexões de cliente abaixo dessa largura de banda.

Por padrão, o valor limite é de 2147483647 kilobits por segundo.

As seguintes configurações de política estão relacionadas:

- Valor limite de compressão progressiva
- Compressão progressiva pesada

#### TAXA DE QUADROS MÍNIMA ALVO

Esta configuração especifica a taxa de quadros mínima por segundo que o sistema tenta manter, para imagens dinâmicas, em condições de baixa largura de banda.

Por padrão, isso é definido como 10fps.

Para as versões 7.0 a 7.6 do VDA, esta configuração se aplica somente quando o modo gráfico herdado está ativado. Para as versões 7.6 FP1 e posteriores do VDA, esta configuração se aplica quando o modo gráfico herdado está desativado ou ativado.

> **Observação:**
>
> A política de taxa de quadros mínima de destino foi preterida e está definida como 10 fps. Isso pode ser alterado pelos usuários finais usando o controle deslizante de Qualidade no indicador de status gráfico.

### Configurações de política de imagens estáticas

A seção **Imagens Estáticas** contém configurações que permitem remover ou alterar a compactação para imagens estáticas.

#### COMPACTAÇÃO DE COR EXTRA

Esta configuração habilita ou desabilita o uso de compactação de cor extra em imagens entregues por conexões de cliente com largura de banda limitada, melhorando a capacidade de resposta ao reduzir a qualidade das imagens exibidas.

Por padrão, a compactação de cor extra está desabilitada.

Quando habilitada, a compactação extra de cores é aplicada somente quando a largura de banda da conexão do cliente está abaixo do valor limite de compactação extra de cores. Quando a largura de banda da conexão do cliente está acima do valor limite ou a opção Desabilitado é selecionada, a compactação extra de cores não é aplicada.

#### LIMITE DE COMPACTAÇÃO DE COR EXTRA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Modo gráfico herdado está habilitada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão abaixo da qual a compactação extra de cores é aplicada. Se a largura de banda da

conexão do cliente cair abaixo do valor definido, a compactação extra de cores, se habilitada, será aplicada.

Por padrão, o valor limite é de 8192 kilobits por segundo.

### COMPACTAÇÃO PESADA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Modo gráfico herdado está habilitada.

Esta configuração habilita ou desabilita a redução da largura de banda além da compactação progressiva sem perda de qualidade da imagem, usando um algoritmo gráfico mais avançado, mas que exige mais da CPU.

Por padrão, a compactação pesada está desabilitada.

Se habilitada, a compactação pesada se aplica a todas as configurações de compactação com perdas. Ela é suportada no aplicativo Citrix Workspace™ mas não tem efeito em outros plug-ins.

As seguintes configurações de política estão relacionadas:

- Nível de compressão progressiva
- Valor limite de compressão progressiva

### NÍVEL DE COMPRESSÃO COM PERDAS

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Modo gráfico herdado está ativada.

Esta configuração controla o grau de compressão com perdas usado em imagens entregues por conexões de cliente que são limitadas em largura de banda. Nesses casos, exibir imagens sem compressão pode ser lento.

Por padrão, a compressão média é selecionada.

Para melhorar a capacidade de resposta com imagens que consomem muita largura de banda, use alta compressão. Onde a preservação dos dados da imagem é vital; por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável, você pode não querer usar compressão com perdas.

Configuração de política relacionada: Valor limite de compressão com perdas

### VALOR LIMITE DE COMPRESSÃO COM PERDAS

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política Modo gráfico herdado está ativada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual a compressão com perdas é aplicada.

Por padrão, o valor limite é 2147483647 kilobits por segundo.

Adicionar a configuração Nível de compressão com perdas a uma política e não incluir nenhum limite especificado pode melhorar a velocidade de exibição de bitmaps de alta detalhes, como fotografias, em uma LAN.

Configuração de política relacionada: Nível de compressão com perdas

### Configurações de política de dispositivos WIA

A seção **Dispositivos WIA** inclui configurações de política para gerenciar o redirecionamento de scanner usando a Aquisição de Imagens do Windows (WIA).

#### Redirecionamento WIA

Dispositivos WIA, como câmeras digitais e scanners, se comunicam com aplicativos de processamento de imagem hospedados no servidor usando a estrutura WIA. Esta configuração permite ou proíbe que os usuários acessem dispositivos WIA no dispositivo do usuário. Por padrão, o redirecionamento WIA é proibido.

Para obter informações sobre dispositivos compatíveis com WIA, consulte dispositivos WIA.

## Recursos HDX™ gerenciados pelo registro

> **Observação:**

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

> Para abrir o Editor do Registro, execute `regedit.exe` no servidor. Em seguida, navegar até a chave do registro para adicionar ou editar as configurações.

## Dispositivos

### Teclados Bloomberg

O Citrix Virtual Apps and Desktops™ oferece suporte ao teclado Bloomberg modelo 4 e modelo 3 starboard. Por padrão, o suporte para o teclado Bloomberg aprimorado está desabilitado.

Para habilitar o suporte para o teclado Bloomberg, defina o seguinte valor de registro na máquina cliente antes de iniciar uma conexão:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Nome do valor**: `EnableBloombergHID`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `0` - Desabilitar
  - `1` - Habilitar

Para obter mais informações, consulte Teclado Bloomberg.

### Unidades cliente mapeadas

Como precaução de segurança, quando um usuário faz logon no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades cliente sem permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis localizados em unidades cliente mapeadas, substitua esse padrão editando o registro no servidor.

Para permitir o acesso, edite o seguinte valor de registro (crie **CDMSettings** se não existir):

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **Nome do valor**: `ExecuteFromMappedDrive`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Permitir acesso
  - `0` - Negar acesso em unidades mapeadas

A alteração entra em vigor para as sessões conectadas após a edição do registro.

Citrix Virtual Apps and Desktops 7 2006 é a primeira versão a conter este local de registro. Versões anteriores do Citrix Virtual Apps and Desktops usavam um local de registro diferente.

Para obter mais informações, consulte Mapeamento de Unidade Cliente.

### Canetas Microsoft Surface Pro e Surface Book

O Citrix Virtual Apps and Desktops oferece suporte à funcionalidade padrão de caneta com aplicativos baseados em Windows Ink. Por padrão, esse recurso está ativado.

Para desativar ou ativar esse recurso, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Nome do valor**: `DisablePen`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desabilitar
  - `0` - Habilitar

Para obter mais informações, consulte Canetas Microsoft Surface Pro e Surface Book.

### Lista de permissões de aplicativos do Windows Image Acquisition

Essa configuração permite controlar quais aplicativos no VDA podem acessar o redirecionamento do scanner de Aquisição de Imagem do Windows.

Por padrão, nenhum aplicativo tem acesso à Aquisição de Imagem do Windows.

Para ajustar a Aquisição de Imagem do Windows para aplicativos no VDA, crie a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **Nome do valor**: `WIAAllowedProcesses`

  Selecione e clique com o botão direito do mouse em **WIAAllowedProcesses**. Escolha **Novo > Valor de Cadeia de Caracteres Múltiplas** e renomeie o novo valor para **AllowProcesses**.
- Dados do valor: Insira o caminho completo e o nome do processo para cada aplicativo que pode acessar a Aquisição de Imagem do Windows. Forneça cada aplicativo em uma nova linha.

Quaisquer alterações a essa configuração entrarão em vigor na próxima vez que você iniciar uma sessão no VDA.

## Geral

### HDX Direct

O tempo limite padrão para HDX Direct em hosts de sessão de várias sessões é de 60 segundos. Para alterar o tempo limite, modifique o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\HdxDirect`
- **Nome do valor**: `HdxDirectInitiateTimeoutInSeconds`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `60` (Decimal)

### HDX Reducer

Você pode configurar a versão do algoritmo de compressão HDX (Reducer) que você deseja usar no host da sessão.

Para habilitar o Reducer V4 em um VDA de sessão única, defina o seguinte valor de registro:

**Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **Nome do valor**: `ReducerOverrideMask` **Tipo de valor**: `DWORD` **Dados do valor**: `23` (Decimal)

Para habilitar o Reducer V4 em um VDA de múltiplas sessões, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nome do valor**: `ReducerOverrideMask`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `23` (Decimal)

### Configurar tempo limite de EDT

Você pode configurar o tempo limite de EDT para qualquer valor entre 5 e 25 segundos no VDA. O valor padrão do tempo limite de EDT é de 25 segundos.

- **Chave**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **Tipo de valor**: `DWORD`
- **Nome do valor**: `edtConnectionTimeout`
- **Dados do valor**: tempo em segundos entre 5 e 25 (decimal)

Você também pode configurar o tempo limite para o aplicativo Citrix Workspace™ para Windows:

- **Chave**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **Tipo de valor**: `String / REG_SZ`
- **Nome do valor**: `edtConnectionTimeout`
- **Dados do valor**: tempo em segundos entre 5 e 25 (decimal)

### Configurar a versão do Rendezvous

Para configurar a versão do Rendezvous a ser usada, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **Tipo de valor**: `DWORD`
- **Nome do valor**: `GctRegistration`
- **Dados do valor**:
  - `1` - Para habilitar V2
  - `0` - Para habilitar V1

### Configurar logon automático no VDA

Essa configuração permite habilitar ou desabilitar a configuração de política da Microsoft **Sempre solicitar senha** nos VDAs de SO de sessão única e SO de várias sessões do Windows 10.

Se **Sempre solicitar senha** estiver habilitado, os usuários devem inserir as credenciais no VDA ao iniciar uma sessão remota. Se essa configuração estiver desabilitada, os usuários se conectarão automaticamente à sessão remota sem fornecer credenciais no VDA.

Por padrão, a configuração de política da Microsoft está desabilitada. Para habilitar ou desabilitar a configuração **Sempre solicitar senha**, defina o seguinte valor de registro no VDA:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **Nome do valor**: `AutoLogon`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desabilita a configuração de política da Microsoft e permite que os usuários façam login automaticamente em uma sessão remota.

- `0` – Habilita a configuração de política da Microsoft e solicita que os usuários forneçam credenciais ao iniciar uma sessão remota.

**Desabilitar aviso de tempo limite**

Por padrão, os usuários com sessões inativas ou ociosas recebem uma mensagem de aviso dois minutos antes que a sessão seja desconectada automaticamente.

Essa configuração desabilita e remove a mensagem de aviso para usuários que atingem o limite de tempo limite de sessão ociosa nos seguintes:

- Windows Server 2004
- Windows 10 multi-session 2004 ou SO de várias sessões posterior

Para remover o aviso, defina o seguinte valor de registro no VDA:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **Nome do valor**: `fEnableTimeoutWarning`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desativar a mensagem de aviso
  - `0` - Ativar a mensagem de aviso

Para exibir a mensagem de aviso, exclua o valor do registro ou defina-o como `0`.

**Descoberta de MTU do EDT**

A Descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso evita a fragmentação de pacotes EDT que pode resultar em degradação do desempenho ou falha ao estabelecer uma sessão.

Essa configuração é habilitada por padrão. Para desativar a Descoberta de MTU do EDT, configure o seguinte valor de registro e reinicie o VDA.

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nome do valor**: `MtuDiscovery`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Essa configuração é válida para toda a máquina e afeta todas as sessões que se conectam de um cliente compatível.

#### Habilitar modo tolerante a perdas

Você pode acessar o áudio adaptável usando o modo tolerante a perdas para o serviço de áudio bidirecional para Citrix Workspace app para Windows, VDA multiusuário e VDA de desktop. Essa configuração está desabilitada por padrão. Para habilitar o modo tolerante a perdas, dependendo da máquina que você está usando, configure o seguinte valor de registro e reinicie a máquina respectiva.

Para o cliente Citrix Workspace app para Windows,

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nome do valor**: `EdtUnreliableAllowed`
- **Tipo de valor**: `REG_SZ`
- **Dados do valor**: `1`

Para TS VDA,

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio`
- **Nome do valor**: `EdtUnreliableAllowed`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para WS VDA,

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio`
- **Nome do valor**: `EdtUnreliableAllowed`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

### Redirecionamento geral de conteúdo

#### Adicionar tipos de URL para redirecionamento do host para o cliente

Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL: HTTP, HTTPS, RTSP, RTSPU, PNM e MMS. Você pode adicionar tipos de URL à lista criando as seguintes chaves e valores de registro no cliente Windows.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **Nome do valor**: `ExtraURLProtocols`
- **Tipo de valor**: `REG_SZ`
- **Dados do valor**: Especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade da URL. Por exemplo: `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL apenas para clientes Windows. Clientes que não possuem essa configuração de registro rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para manipular os tipos de URL especificados.

Para obter mais informações, consulte Redirecionamento do host para o cliente.

#### Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Considere que você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo do usuário. Nesse caso, a parte do volume local especificada pelo usuário é redirecionada.

Para habilitar o redirecionamento de pasta do cliente no servidor, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **Nome do valor**: `CFROnlyModeAvailable`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para obter mais informações, consulte Redirecionamento de pasta do cliente.

#### Redirecionamento do host para o cliente para um conjunto específico de sites

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, defina o seguinte valor de registro no VDA do servidor.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nome do valor**: `ValidSites`
- **Tipo de valor**: `REG_MULTI_SZ`

- **Dados do valor**: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Esse curinga corresponde a um único nível de domínio, o que é consistente com as regras no RFC 6125. Por exemplo:

`www.example.com`

`*.example.com`

Para obter mais informações, consulte Redirecionamento do host para o cliente.

#### Comportamento do aplicativo local ao fazer logoff e desconectar

Por padrão, os aplicativos locais continuam a ser executados quando um usuário faz logoff ou se desconecta da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual. Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, defina o seguinte valor de registro na área de trabalho hospedada:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **Nome do valor**: `Session State`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Os aplicativos locais continuam a ser executados quando um usuário faz logoff ou se desconecta da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.
  - `3` - Os aplicativos locais são fechados quando um usuário faz logoff ou se desconecta da área de trabalho virtual.

Para obter mais informações, consulte Acesso a aplicativos locais e redirecionamento de URL.

#### Remover tipos de URL da lista padrão para redirecionamento do host para o cliente

Para remover tipos de URL da lista de redirecionamento padrão, crie as seguintes chaves e valores de registro no VDA do servidor.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nome do valor**: `DisableServerFTA`

- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`
- **Nome do valor**: `NoRedirectClasses`
- **Tipo de valor**: `REG_MULTI_SZ`
- **Dados do valor**: Especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

`http`

`https`

`rtsp`

Para obter mais informações, consulte Redirecionamento do host para o cliente.

### Configuração padrão do navegador do VDA do servidor

Você pode habilitar o redirecionamento do host para o cliente para substituir qualquer configuração de navegador padrão no VDA do Servidor. Se um URL da web não for redirecionado, o iniciador Citrix passa o URL para o navegador configurado na chave de registro `command_backup`. Por padrão, a chave aponta para o Internet Explorer, mas você pode modificá-la para incluir o caminho para um navegador diferente.

- Internet Explorer (Padrão)
  - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
- Google Chrome
  - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nome do valor**: `Default`

    - **Tipo de valor**: `REG_SZ`
    - **Dados do valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
    - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - **Nome do valor**: `Default`
    - **Tipo de valor**: `REG_SZ`
    - **Dados do valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- Microsoft Edge
    - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
    - **Nome do valor**: `Default`
    - **Tipo de valor**: `REG_SZ`
    - **Dados do valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
    - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - **Nome do valor**: `Default`
    - **Tipo de valor**: `REG_SZ`
    - **Dados do valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

### O Acesso a Aplicativos Locais para aplicativos publicados

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada, sem alternar de uma área de trabalho para outra. Para fornecer acesso a aplicativos publicados, defina o seguinte valor de registro no servidor:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **Nome do valor**: `ClientHostedAppsEnabled`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
    - `1` - Habilitar
    - `0` - Desabilitar

Para obter mais informações, consulte Acesso a aplicativos locais e redirecionamento de URL.

## Gráficos

### Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário está desabilitada por padrão.

Para usar os recursos POC de aceleração CUDA, habilite a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Nome do valor**: `CUDA`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `00000001`

Para usar os recursos POC de aceleração OpenCL, habilite a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Nome do valor**: `OpenCL`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `00000001`

Para obter mais informações, consulte Aceleração de GPU para SO de múltiplas sessões do Windows

### Modo progressivo

O modo progressivo é desabilitado por padrão. Você pode alterar o estado do modo progressivo com o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **Tipo de valor**: `REG_DWORD`
- **Nome do valor**: `ProgressiveDisplay`
- **Dados do valor**:

- `0` - Sempre desativado (Desabilita o modo progressivo. Este valor é o padrão.)
- `1` - Automático (Alterna com base nas condições da rede.)
- 2 = Sempre ativado

Para obter mais informações, consulte Modo progressivo.

> **Observação:**
>
> O modo progressivo foi preterido. O Thinwire é uma opção alternativa que otimiza a entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

### Renderização do Windows Presentation Foundation (WPF)

O HDX 3D Pro permite que aplicativos com muitos gráficos executados em sessões do Windows Multi-session OS sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor.

Para habilitar a renderização de aplicativos WPF usando a GPU do servidor, crie a seguinte configuração no registro do servidor que executa o Windows multi-session OS:

1. Abra o Editor do Registro no VDA e vá para a seguinte chave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Crie ou edite os seguintes valores de registro:

   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - Flag = 0x00000412
   - WPF = 0x00000001

3. Crie uma subchave com o nome executável do seu aplicativo WPF. Por exemplo, se seu aplicativo for chamado de "mywpfapp.exe”, crie a seguinte chave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Reinicie o servidor para que a configuração entre em vigor.

Para obter mais informações, consulte Aceleração de GPU para Windows multi-session OS e o blog sobre Como obter o melhor dos aplicativos WPF no Windows multi-session OS.

## Multimídia

### Evitar eco durante conferências multimídia

O Citrix Virtual Apps and Desktops fornece uma opção de cancelamento de eco que minimiza qualquer eco. Este recurso é habilitado por padrão. Para desabilitar o cancelamento de eco, você pode alterar uma das seguintes configurações de registro:

- **Chave**:
  - 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nome do valor**: `EchoCancellation`
- **Tipo de valor**: `String/REG_SZ`
- **Dados do valor**: `False`

Para obter mais informações, consulte Recursos de áudio.

### Limitação de áudio

Depois de instalar um dispositivo de áudio no seu cliente, habilitar o redirecionamento de áudio e iniciar uma sessão RDS, os arquivos de áudio podem não reproduzir som. Como solução alternativa, adicione a seguinte chave de registro na máquina RDS e reinicie a máquina:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **Nome do valor**: `EnableSvchostMitigationPolicy`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Para obter mais informações, consulte Recursos de áudio.

### Resolução de webcam de alta definição

Se a negociação do tipo de mídia falhar, o HDX retorna para a resolução VGA padrão (640 x 480 pixels). Você pode usar chaves de registro no cliente para configurar a resolução padrão. Antes de

definir as seguintes chaves de registro, certifique-se de que a câmera suporte a resolução especificada.

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- Largura
  - **Nome do valor**: `DefaultWidth`
  - **Tipo de valor**: `DWORD`
  - **Dados do valor**: largura desejada em decimal (por exemplo: 1280)
- Altura
  - **Nome do valor**: `DefaultHeight`
  - **Tipo de valor**: `DWORD`
  - **Dados do valor**: altura desejada em decimal (por exemplo 720)

**Modo de fallback do Microsoft Teams**

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Não Conectado" em Teams/Sobre/Versão), o VDA retorna para tecnologias HDX legadas, como redirecionamento de webcam e redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão do aplicativo Workspace/SO de plataforma que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam.

Para controlar o mecanismo de fallback, defina um dos seguintes valores de registro no VDA:

- **Chave** (apenas uma é necessária):
  - **Configuração do computador:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **Configuração do usuário:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **Nome do valor**: `DisableFallback`
- **Tipo de valor**: `DWORD`
- Dados do valor:
  - `1` - Desativar modo de fallback
  - `2` - Ativar somente áudio

Se o valor não estiver presente ou estiver definido como 0, o modo de fallback será ativado. Este recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior. Para obter mais informações, consulte Otimização para Microsoft Teams.

### Otimização para Microsoft Teams com Citrix App Layering™

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, crie uma chave de registro vazia chamada **PortICA** no Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Mantenha o nome, tipo e dados do valor padrão.

- Chave para a versão de 32 bits do Editor do Registro: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- Chave para a versão de 64 bits do Editor do Registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

Para obter mais informações, consulte Otimização para Microsoft Teams.

### Compactação de software da webcam

Se uma webcam suportar codificação de hardware, a compactação de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compactação de software, adicione os seguintes valores ao cliente:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **Nome do valor**: `DeepCompress_ForceSWEncode`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

### Compressão de vídeo da webcam

A compressão de vídeo da webcam HDX envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compressão de webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Este recurso é habilitado por padrão.

Para desabilitar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina o seguinte valor de registro no VDA.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **Nome do valor**: `OfferH264ToApp`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

#### Taxa de quadros da compressão de vídeo da webcam

Para ajustar a taxa de quadros de vídeo preferencial, edite o seguinte valor de registro no cliente:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **Nome do valor**: `FramesPerSecond`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `15`

Se a webcam não suportar a taxa de quadros especificada, o aplicativo usará 15 FPS por padrão.

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

## Configurações de política de gerenciamento de carga

A seção **Gerenciamento de Carga** inclui configurações de política para habilitar e configurar o gerenciamento de carga entre servidores que fornecem máquinas Windows Multi-session OS.

Para obter informações sobre como calcular o índice do avaliador de carga, consulte CTX202150.

### Tolerância de logon simultâneo

Esta configuração especifica o número máximo de logons simultâneos que um servidor pode aceitar.

Por padrão, este valor é definido como 2.

Quando esta configuração está habilitada, o balanceamento de carga tenta evitar ter mais do que o número especificado de logons ativos em um VDA de Servidor ao mesmo tempo. No entanto, o limite não é estritamente imposto. Para impor o limite (e fazer com que os logons simultâneos que excedem o número especificado falhem), crie a seguinte chave de registro:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit Type: DWORD Value: 1

### Uso da CPU

Esta configuração especifica o nível de uso da CPU, em porcentagem, no qual o servidor relata uma carga total. Quando habilitado, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, esta configuração está desabilitada e o uso da CPU é excluído dos cálculos de carga.

### Prioridade de processo excluída do uso da CPU

> **Observação:**
>
> Em cenários onde o Workspace Environment Management gerencia máquinas, usar esta configuração juntamente com as configurações de Prioridade da CPU pode ter resultados indesejados. Recomendamos que você desabilite esta configuração se optar por usar as configurações de Prioridade da CPU.

> Esta configuração especifica o nível de prioridade no qual o uso da CPU de um processo é excluído do índice de carga de Uso da CPU.

Por padrão, este valor é definido como **Abaixo do Normal** ou **Baixo**.

### Uso de disco

Esta configuração especifica o comprimento da fila de disco no qual o servidor relata uma carga total de 75%. Quando habilitado, o valor padrão para o comprimento da fila de disco é 8.

Por padrão, esta configuração está desabilitada e o uso do disco é excluído dos cálculos de carga.

### Número máximo de sessões

Esta configuração especifica o número máximo de sessões que um servidor pode hospedar. Quando ativada, a configuração padrão para o número máximo de sessões que um servidor pode hospedar é 250.

Por padrão, esta configuração está ativada.

### Uso de memória

Esta configuração especifica o nível de uso da memória, em porcentagem, no qual o servidor relata uma carga total. Quando ativada, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, esta configuração está desativada e o uso da memória é excluído dos cálculos de carga.

### Carga base de uso da memória

Esta configuração especifica uma aproximação do uso da memória do sistema operacional base. Além disso, define, em MB, o uso da memória abaixo do qual um servidor é considerado com carga zero.

Por padrão, este valor é definido como 768 MB.

## Configurações de política de gerenciamento de perfil

### Configurações avançadas de política

#### Número de tentativas ao acessar arquivos bloqueados

Define o número de tentativas ao acessar arquivos bloqueados.

Se esta política estiver desabilitada, o valor padrão de cinco tentativas será usado. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o valor padrão será usado.

#### Processar arquivos de cookies da Internet ao fazer logoff

Algumas implantações deixam cookies de Internet extras que `Index.dat` não referencia. Os cookies extras deixados no sistema de arquivos após navegação contínua podem levar ao inchaço do perfil. Esta política permite habilitar o Profile Management para forçar o processamento de Index.dat e remover os cookies extras. A política aumenta os tempos de logoff, então habilite-a somente depois de experimentar esse problema.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui nem no arquivo .ini, nenhum processamento de Index.dat ocorrerá.

#### Desabilitar configuração automática

O Profile Management examina qualquer ambiente Citrix Virtual Desktops™, por exemplo, para a presença de vDisks pessoais, e configura a Política de Grupo de acordo. Somente as políticas do Profile Management no estado Não Configurado são ajustadas, de modo que quaisquer personalizações que você tenha feito são preservadas.

Esta política permite acelerar a implantação e simplifica a otimização. Você não precisa configurar esta política. No entanto, você pode desabilitar a configuração automática ao fazer uma das seguintes ações:

- Atualizar para reter configurações de versões anteriores
- Solução de problemas

Você pode considerar a configuração automática como um verificador de configuração dinâmica que configura automaticamente as configurações de política padrão de acordo com os ambientes em tempo de execução. Isso elimina a necessidade de configurar as configurações manualmente. Os ambientes de tempo de execução incluem:

- Windows
- Versões do sistema operacional Windows
- Presença de Citrix Virtual Desktops
- Presença de vDisks pessoais

A configuração automática pode alterar as seguintes políticas se o ambiente mudar:

- Gravação ativa
- Sempre armazenar em cache
- Excluir perfis armazenados em cache localmente no logoff
- Atraso antes de excluir perfis armazenados em cache
- Streaming de perfil

Consulte a tabela a seguir para o status padrão das políticas em diferentes sistemas operacionais:

| | SO MULTISSESSÃO | SO DE SESSÃO ÚNICA |
|---|---|---|
| Gravação ativa | Ativado | *Desabilitado* se o vDisk Pessoal estiver em uso; caso contrário, habilitado. |
| Sempre armazenar em cache | Desabilitado | *Desabilitado* se o vDisk Pessoal estiver em uso; caso contrário, habilitado. |
| Excluir perfis armazenados em cache localmente no logoff | Ativado | *Desabilitado* se uma das seguintes situações ocorrer: vDisk Pessoal estiver em uso, Citrix Virtual Desktops estiver atribuído ou Citrix Virtual Desktops não estiver |

| | SO MULTISSESSÃO | SO DE SESSÃO ÚNICA |
|---|---|---|
| | | instalado; caso contrário, habilitado. |
| Atraso antes de excluir perfis armazenados em cache | 0 segundos | 60 segundos se as alterações do usuário não forem persistentes; caso contrário, 0 segundos. |
| Streaming de perfil | Ativado | *Desabilitado* se o Personal vDisk estiver em uso; caso contrário, habilitado. |

No entanto, com a configuração automática desabilitada, todas as políticas acima são padronizadas para **Desabilitado**.

> **Importante:**
>
> O Personal vDisk foi descontinuado. Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

> A partir do Profile Management 1909, você pode ter uma experiência aprimorada com o menu Iniciar no Windows 10 (versão 1607 e posterior) e no Windows Server 2016 e posterior. Essa melhoria é alcançada por meio da configuração automática das seguintes políticas:

- Adicione `Appdata\Local\Microsoft\Windows\Caches` e `Appdata\Local\Packages` a **Pastas para Espelhar**.
- Adicione `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` a **Arquivos para sincronizar**.

Se essa configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se essa configuração não for configurada aqui nem no arquivo .ini, a configuração automática será ativada. Nesse caso, as configurações do Profile Management podem mudar se o ambiente mudar.

### Fazer logoff do usuário se um problema for encontrado

Permite especificar se o Profile Management faz logoff dos usuários se um problema for encontrado.

Se esta política estiver desabilitada ou não configurada, o Profile Management fornece um perfil temporário aos usuários se um problema for encontrado. Por exemplo, o armazenamento de usuário está indisponível.

Se estiver habilitado, uma mensagem de erro será exibida e os usuários serão desconectados. Essa configuração pode simplificar a solução de problemas.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui nem no arquivo .ini, um perfil temporário será fornecido.

### Programa de Melhoria da Experiência do Cliente

Por padrão, o Programa de Melhoria da Experiência do Cliente é ativado para ajudar a melhorar a qualidade e o desempenho dos produtos Citrix® coletando estatísticas anônimas e dados de uso.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

### Habilitar roaming do índice de pesquisa para o Outlook

Permite a experiência de pesquisa do Outlook baseada no usuário, fazendo o roaming automático dos dados de pesquisa do Outlook junto com o perfil do usuário. Este recurso requer espaço extra no armazenamento do usuário para armazenar os índices de pesquisa do Outlook.

Faça logoff e, em seguida, faça logon novamente para que esta política entre em vigor.

### Banco de dados do índice de pesquisa do Outlook – backup e restauração

Permite especificar o que o Profile Management faz durante o logon quando a política Habilitar roaming do índice de pesquisa para Outlook está ativada.

Se esta política estiver ativada, o Profile Management faz backup do banco de dados do índice de pesquisa cada vez que o banco de dados é montado com sucesso no logon. O Profile Management trata o backup como a cópia íntegra do banco de dados do índice de pesquisa. Quando uma tentativa de montar o banco de dados do índice de pesquisa falha devido à corrupção do banco de dados, o Profile Management reverte o banco de dados do índice de pesquisa para a última cópia íntegra conhecida.

> Nota:

> O Profile Management exclui o backup salvo anteriormente depois que um novo backup é salvo com sucesso. O backup consome o armazenamento VHDX disponível.

### HABILITAR SUPORTE A SESSÕES SIMULTÂNEAS PARA ROAMING DE DADOS DE PESQUISA DO OUTLOOK

Permite que o Profile Management forneça uma experiência de pesquisa nativa do Outlook em sessões simultâneas do mesmo usuário. Use esta política com a política de roaming do índice de pesquisa para Outlook.

Com esta política ativada, cada sessão simultânea usa um arquivo OST do Outlook separado.

Por padrão, apenas dois discos VHDX podem ser usados para armazenar arquivos OST do Outlook (um arquivo por disco). Se o usuário iniciar mais sessões, seus arquivos OST do Outlook serão armazenados no perfil de usuário local. Você pode especificar o número máximo de discos VHDX para armazenar arquivos OST do Outlook.

### HABILITAR CONTÊINER DO ONEDRIVE

Permite que as pastas do OneDrive sejam transferidas com os usuários.

O contêiner do OneDrive é uma solução de roaming de pasta baseada em VHDX. O Profile Management cria um arquivo VHDX por usuário em um compartilhamento de arquivos e armazena as pastas do OneDrive dos usuários nos arquivos VHDX. Os arquivos VHDX são anexados quando os usuários fazem logon e desanexados quando os usuários fazem logoff.

### Roaming de aplicativos UWP

Permite habilitar que aplicativos UWP (Universal Windows Platform) sejam transferidos com os usuários. Como resultado, os usuários podem acessar os mesmos aplicativos UWP de diferentes dispositivos.

Com esta política ativada, o Profile Management permite que os aplicativos UWP sejam transferidos com os usuários, armazenando os aplicativos em discos VHDX separados. Esses discos são anexados durante os logons dos usuários e desanexados durante os logoffs dos usuários.

Precedência da configuração:

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não for configurada nem aqui nem no arquivo .ini, este recurso será desativado.

### HABILITAR PROCESSAMENTO ASSÍNCRONO PARA A POLÍTICA DE GRUPO DO USUÁRIO NO LOGON

O Windows oferece dois modos de processamento para a Política de Grupo do usuário: síncrono e assíncrono. O Windows usa um valor de registro para determinar o modo de processamento para o próximo logon do usuário. Se o valor de registro não existir, o modo síncrono será aplicado. O valor de registro é uma configuração de nível de máquina e não é transferido com os usuários. Assim, o modo assíncrono não será aplicado como esperado se os usuários:

- Fizerem logon em máquinas diferentes.
- Fizerem logon na mesma máquina onde a política Excluir perfis armazenados em cache localmente no logoff está ativada.

Com esta política ativada, o valor de registro é transferido com os usuários. Como resultado, o modo de processamento é aplicado cada vez que os usuários fazem logon.

### PROPORÇÃO DE ESPAÇO LIVRE PARA ACIONAR A COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar a proporção de espaço livre para acionar a compactação de disco VHD. Quando a proporção de espaço livre excede o valor especificado no logoff do usuário, a compactação de disco é acionada.

Proporção de espaço livre = (tamanho atual do arquivo VHD – tamanho mínimo necessário do arquivo VHD*) ÷ tamanho atual do arquivo VHD

* Obtido usando o método GetSupportedSize da classe `MSFT_Partition` do sistema operacional Microsoft Windows.

### NÚMERO DE LOGOFFS PARA ACIONAR A COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar o número de logoffs de usuário para acionar a compactação de disco VHD.

Quando o número de logoffs desde a última compactação atinge o valor especificado, a compactação de disco é acionada novamente.

### DESABILITAR DESFRAGMENTAÇÃO PARA COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar se a desfragmentação de arquivos deve ser desabilitada para a compactação de disco VHD.

Quando a compactação de disco VHD está habilitada, o arquivo de disco VHD é primeiro desfragmentado automaticamente usando a ferramenta `defrag` interna do Windows e, em seguida, compactado. A desfragmentação de disco VHD produz melhores resultados de compactação, enquanto desabilitá-la pode economizar recursos do sistema.

### Habilitar gravação de várias sessões para contêineres de perfil

Habilita a gravação para contêineres de perfil em cenários de várias sessões. Se habilitado, as alterações em todas as sessões são gravadas de volta nos contêineres de perfil. Caso contrário, apenas as alterações na primeira sessão são salvas porque apenas a primeira sessão está no modo de leitura/gravação nos contêineres de perfil. Os contêineres de perfil do Citrix Profile Management são suportados a partir do Citrix Profile Management 2103. O FSLogix Profile Container é suportado a partir do Citrix Profile Management 2003.

Para usar esta política para o FSLogix Profile Container, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O recurso FSLogix Profile Container está instalado e habilitado.
- O tipo de perfil está definido como **Tentar perfil de leitura-gravação e fallback para somente leitura** no FSLogix.

### Replicar armazenamentos de usuário

Permite replicar o armazenamento de perfil de usuário remoto para vários caminhos em cada logon e logoff. Isso permite que o Profile Management forneça redundância de perfil para logons de usuário.

Habilitar a política aumenta a E/S do sistema e pode prolongar os logoffs.

> **Observação:**
>
> - Este recurso está disponível tanto para o armazenamento de usuário quanto para o contêiner de perfil completo.
> - Contêineres de perfil replicados fornecem redundância de perfil para logons de usuário, mas não para failover em sessão.

### Habilitar acesso baseado em credenciais a armazenamentos de usuário

Por padrão, o Citrix Profile Management personifica o usuário atual para acessar o armazenamento de usuário. Habilite este recurso se você não quiser que o Profile Management personifique o usuário atual ao acessar o armazenamento de usuário. Você pode colocar os armazenamentos de usuário em repositórios de armazenamento (por exemplo, Azure Files) aos quais o usuário atual não tem permissão para acessar.

Para garantir que o Profile Management possa acessar os armazenamentos de usuário, salve as credenciais do servidor de armazenamento de perfil no Workspace Environment Management™ (WEM) ou no Gerenciador de Credenciais do Windows. Recomendamos que você use o Workspace Environment Management para eliminar a necessidade de configurar as mesmas credenciais para cada máquina onde o Profile Management é executado. Se você usar o Gerenciador de Credenciais do Windows, use a conta do Sistema Local para salvar as credenciais com segurança.

> **Observação:**

> Esta política está disponível para armazenamentos de usuário baseados em arquivo e baseados em VHDX. Para versões do Profile Management anteriores a 2212, esta política está disponível apenas para armazenamentos de usuário baseados em VHDX.

> Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não for configurada nem aqui nem no arquivo .ini, ela será desabilitada por padrão.

### Personalizar caminho de armazenamento para arquivos VHDX

O Profile Management fornece as seguintes políticas baseadas em VHDX: Contêiner de perfil, Roaming de índice de pesquisa para Outlook e Acelerar espelhamento de pasta. Por padrão, os arquivos VHDX são armazenados no armazenamento de usuário. Esta política permite especificar um caminho separado para armazená-los.

### Capacidade padrão de contêineres VHD

Permite especificar a capacidade de armazenamento padrão (em GB) dos contêineres VHD.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui nem no arquivo .ini, o padrão é 50 (GB).

### Reconectar automaticamente discos VHDX em sessões

Com esta política ativada, o Profile Management garante um alto nível de estabilidade das políticas baseadas em VHDX. Por padrão, esta política está ativada.

Quando esta política está ativada, o Profile Management monitora os discos VHDX que estão em uso por políticas baseadas em VHDX. Se algum dos discos for desanexado, o Profile Management o reconecta automaticamente.

### Limite de expansão automática do contêiner de perfil

Permite especificar a porcentagem de utilização da capacidade de armazenamento na qual os contêineres de perfil acionam a expansão automática.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui ou no arquivo .ini, o padrão é 90 (%) da capacidade de armazenamento.

### Incremento de expansão automática do contêiner de perfil

Permite especificar a quantidade de capacidade de armazenamento (em GB) pela qual os contêineres de perfil se expandem automaticamente quando a expansão automática é acionada.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui nem no arquivo .ini, o padrão é 10 (GB).

### Limite de expansão automática do contêiner de perfil

Permite especificar a capacidade máxima de armazenamento (em GB) para a qual os contêineres de perfil podem se expandir automaticamente quando a expansão automática é acionada.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui nem no arquivo .ini, o padrão é 80 (GB).

### Habilitar configurações de política de nível de usuário

Com esta política habilitada, as configurações de política de nível de máquina podem funcionar no nível do usuário, e as configurações de nível de usuário substituem as configurações de nível de máquina.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui nem no arquivo .ini, ela será desabilitada.

### Definir ordem de prioridade para grupos de usuários

Permite especificar a ordem de prioridade para grupos de usuários. A ordem determina qual grupo tem precedência quando um usuário pertence a vários grupos com diferentes configurações de política.

Quando um usuário pertence a vários grupos com configurações de política conflitantes, considere o seguinte:

- Se o usuário pertencer a um ou mais grupos definidos nesta política, o grupo com a maior prioridade terá precedência.
- Se o usuário não pertencer a nenhum dos grupos definidos nesta política, o grupo com o SID listado primeiro em ordem alfabética terá precedência.

### Método de seleção do armazenamento de usuário

Permite especificar o método de seleção do armazenamento de usuário quando vários armazenamentos de usuário estão disponíveis. As opções incluem:

- **Ordem de configuração.** O Profile Management seleciona o armazenamento configurado mais cedo.
- **Desempenho de acesso.** O Profile Management seleciona o armazenamento com o melhor desempenho de acesso.

Precedência de configuração:

1. Se esta configuração não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta configuração não estiver configurada aqui ou no arquivo .ini, **Ordem de configuração** será usada.

## Configurações básicas de política

Esta seção contém configurações de política relacionadas à configuração básica do Profile Management.

### Habilitar Profile Management

Por padrão, para facilitar a implantação, o Profile Management não processa logons ou logoffs. Habilite o Profile Management somente após realizar todas as outras tarefas de configuração e testar o desempenho dos perfis de usuário Citrix® em seu ambiente.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o Profile Management não processará os perfis de usuário do Windows de forma alguma.

### Grupos processados

Podem ser usados grupos locais do computador e grupos de domínio (locais, globais e universais). Os grupos de domínio devem ser especificados no formato: NOME DO DOMÍNIO\NOME DO GRUPO.

Se esta política estiver configurada aqui, o Profile Management processará apenas os membros desses grupos de usuários. Se esta política estiver desabilitada, o Profile Management processará todos os usuários. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, os membros de todos os grupos de usuários serão processados.

### Grupos excluídos

Você pode usar grupos locais do computador e grupos de domínio (locais, globais e universais) para evitar que perfis de usuário específicos sejam processados. Especifique os grupos de domínio no formato NOME DO DOMÍNIO\ NOME DO GRUPO.

Se esta configuração estiver configurada aqui, o Profile Management excluirá os membros desses grupos de usuários. Se esta configuração estiver desabilitada, o Profile Management não excluirá nenhum usuário. Se esta configuração não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não estiver configurada aqui ou no arquivo .ini, nenhum membro de nenhum grupo será excluído.

### Processar logons de administradores locais

Especifica se os logons de membros do grupo BUILTIN\Administrators são processados. Considere que esta política está desabilitada ou não configurada em sistemas operacionais multi-sessão, como ambientes Citrix Virtual Apps. Neste caso, o Profile Management assume que os logons de usuários de domínio, mas não de administradores locais, devem ser processados. Em sistemas operacionais de sessão única (como ambientes Citrix Virtual Desktops), os logons de administrador local são processados. Esta política permite que usuários de domínio com direitos de administrador local, tipicamente usuários do Citrix Virtual Desktops com desktops virtuais atribuídos, possam:

- Ignorar qualquer processamento
- Fazer logon
- Solucionar problemas do desktop que está com problemas no Profile Management

Nota: Os logons de usuários de domínio podem estar sujeitos a restrições impostas pela associação a grupos, geralmente para garantir a conformidade com o licenciamento do produto. Se esta política estiver desabilitada, o Profile Management não processa logons de administradores locais. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, os administradores não serão processados.

### Caminho para o armazenamento do usuário

Define o caminho para o diretório (o armazenamento do usuário) no qual as configurações do usuário (alterações de registro e arquivos sincronizados) são salvas.

O caminho pode ser:

- Um caminho relativo. Ele deve ser relativo ao diretório inicial (que é tipicamente configurado como o atributo #homeDirectory# para um usuário no Active Directory).
- Um caminho UNC. Ele geralmente especifica um compartilhamento de servidor ou um namespace DFS.
- Desabilitado ou não configurado. Neste caso, um valor de #homeDirectory#\Windows é assumido.

Os seguintes tipos de variáveis podem ser usados para esta política:

- Variáveis de ambiente do sistema entre sinais de porcentagem (por exemplo, %ProfVer%). As variáveis de ambiente do sistema geralmente exigem configuração adicional.
- Atributos do objeto de usuário do Active Directory entre sinais de hash (por exemplo, #sAMAccountName#).
- Variáveis do Profile Management. Para obter mais informações, consulte o documento do produto Variáveis do Profile Management.

Variáveis de ambiente do usuário não podem ser usadas, exceto para `%username%` e `%userdomain%`. Você também pode criar atributos personalizados para definir variáveis organizacionais como localização ou usuários completamente. Os atributos diferenciam maiúsculas de minúsculas.

Exemplos:

- `\\server\share#sAMAccountName#` armazena as configurações do usuário no caminho UNC `\\server\share\JohnSmith` (se #sAMAccountName# resolver para JohnSmith para o usuário atual)

- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!` pode se expandir para `\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`

Importante: Quaisquer que sejam os atributos ou variáveis que você usar, verifique se esta política se expande para a pasta um nível acima da pasta que contém NTUSER.DAT. Por exemplo, se este arquivo estiver contido em `\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`, defina o caminho para o armazenamento de usuário como `\\server\profiles$\JohnSmith.Finance\Win8x64` (não a subpasta \UPM_Profile).

Para obter mais informações sobre como usar variáveis ao especificar o caminho para o armazenamento de usuário, consulte os seguintes tópicos:

- Compartilhar perfis de usuário Citrix em vários servidores de arquivos
- Administrar perfis dentro e entre UOs
- Alta disponibilidade e recuperação de desastres com o Profile Management

Se o Caminho para o armazenamento de usuário estiver desativado, as configurações do usuário serão salvas no subdiretório do Windows do diretório inicial.

Se esta política estiver desativada, as configurações do usuário serão salvas no subdiretório do Windows do diretório inicial. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o diretório do Windows na unidade inicial será usado.

**Migrar armazenamento de usuário**

Especifica o caminho para a pasta onde as configurações do usuário (alterações de registro e arquivos sincronizados) foram salvas anteriormente (o caminho do armazenamento de usuário que você usou anteriormente).

Se esta configuração estiver configurada, as configurações do usuário armazenadas no armazenamento de usuário anterior serão migradas para o armazenamento de usuário atual especificado na política "Caminho para o armazenamento de usuário".

O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial.

Em ambos os casos, você pode usar os seguintes tipos de variáveis:

- Variáveis de ambiente do sistema entre sinais de porcentagem
- Atributos do objeto de usuário do Active Directory entre sinais de hash

Exemplos:

- A pasta `Windows\%ProfileVer%` armazena as configurações do usuário em uma subpasta chamada `Windows\W2K3` do armazenamento de usuário (se %ProfileVer% for uma variável de ambiente do sistema que se resolve para W2K3).
- `\\server\share#SAMAccountName#` armazena as configurações do usuário no caminho UNC `\\server\share\<JohnSmith>` (se `#SAMAccountName#` se resolver para JohnSmith para o usuário atual).

No caminho, você pode usar variáveis de ambiente do usuário, exceto `%username%` e `%userdomain%`.

Se esta configuração estiver desabilitada, as configurações do usuário serão salvas no armazenamento de usuário atual.

Se esta configuração não estiver configurada aqui, a configuração correspondente do arquivo .ini será usada.

Se esta configuração não estiver configurada aqui ou no arquivo .ini, as configurações do usuário serão salvas no armazenamento de usuário atual.

**Gravação ativa de volta**

Arquivos e pastas (mas não entradas de registro) que são modificados podem ser sincronizados com o armazenamento de usuário no meio de uma sessão, antes do logoff.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, ela será habilitada.

Suporte a perfil offline

Esta política permite que os perfis sejam sincronizados com o armazenamento de usuário na primeira oportunidade possível. Ela é destinada a usuários de laptop ou dispositivos móveis que fazem roaming. Quando ocorre uma desconexão de rede, os perfis permanecem intactos no laptop ou dispositivo mesmo após reiniciar ou hibernar. À medida que os usuários móveis trabalham, seus perfis são atualizados localmente. Além disso, são eventualmente sincronizados com o armazenamento de usuário quando a conexão de rede é restabelecida.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, os perfis offline serão desabilitados.

### Registro de gravação ativa de volta

Use esta política juntamente com "Gravação ativa de volta". As entradas de registro que são modificadas podem ser sincronizadas com o armazenamento de usuário no meio de uma sessão.

Se você não configurar esta definição aqui, o valor do arquivo .ini será usado.

Se você não configurar esta definição aqui ou no arquivo .ini, o registro de gravação ativa de volta será desabilitado.

#### GRAVAÇÃO ATIVA DE RETORNO NO BLOQUEIO E DESCONEXÃO DA SESSÃO

Com esta política e a política de **Gravação ativa de retorno** ativadas, os arquivos e pastas de perfil são gravados de volta somente quando uma sessão é bloqueada ou desconectada.

Com esta política e as políticas de **Gravação ativa de retorno** e **Gravação ativa de retorno do registro** ativadas, as entradas do registro são gravadas de volta somente quando uma sessão é bloqueada ou desconectada.

### Suporte a perfis offline

Ativa o recurso de perfis offline. Este recurso é destinado a computadores que são frequentemente removidos de redes. Por exemplo, laptops ou dispositivos móveis, não servidores ou desktops.

Se esta definição não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, o suporte a perfis offline será desativado.

## Configurações de política multiplataforma

Esta seção contém configurações de política relacionadas à configuração do recurso de configurações **multiplataforma do Profile Management**.

### Habilitar configurações multiplataforma

Por padrão, para facilitar a implantação, as configurações multiplataforma estão desabilitadas. Ative o processamento habilitando esta política, mas somente após um planejamento e teste completos desse recurso.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

### Grupos de usuários de configurações multiplataforma

Insira um ou mais grupos de usuários do Windows. Por exemplo, você pode usar esta política para processar apenas os perfis de um grupo de usuários de teste. Se esta política estiver configurada, o recurso de configurações multiplataforma do Profile Management processará apenas os membros desses grupos de usuários. Se esta política estiver desabilitada, o recurso processará todos os usuários especificados pela política de grupos processados.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, todos os grupos de usuários serão processados.

### Caminho para definições multiplataforma

Identifica o local de rede dos arquivos de definição que você copiou do pacote de download. Este caminho deve ser um caminho UNC. Os usuários devem ter acesso de leitura a este local, e os administradores devem ter acesso de gravação a ele. O local deve ser um compartilhamento de arquivos Server Message Block (SMB) ou Common Internet File System (CIFS).

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

### Caminho para o armazenamento de configurações multiplataforma

Define o caminho para o armazenamento de configurações multiplataforma, a pasta na qual as configurações multiplataforma dos usuários são salvas. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial.

Esta área é a área comum do armazenamento de usuário onde os dados de perfil compartilhados por várias plataformas estão localizados. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial. Você pode usar as mesmas variáveis que para o **Caminho para o armazenamento de usuário**.

Se esta política estiver desabilitada, o caminho Windows\PM_CP será usado. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o valor padrão será usado.

### Fonte para criar configurações entre plataformas

Especifica uma plataforma como a plataforma base se esta política estiver habilitada na OU dessa plataforma. Esta política migra dados dos perfis da plataforma base para o armazenamento de configurações entre plataformas.

Cada conjunto de perfis de uma plataforma é armazenado em uma OU separada. Você deve decidir quais dados de perfil da plataforma usar para preencher o armazenamento de configurações entre plataformas. É referida como a plataforma base. Considere que o armazenamento de configurações entre plataformas contém um arquivo de definição sem dados, ou que os dados em cache em um perfil de plataforma única são mais recentes do que os dados da definição no armazenamento. Nesse caso, o Gerenciamento de Perfis migra os dados do perfil de plataforma única para o armazenamento, a menos que você desabilite esta política.

> **Importante:**

> Se esta política estiver habilitada em várias OUs, ou em vários objetos de usuário ou máquina, a plataforma na qual o primeiro usuário faz logon se torna o perfil base. Por padrão, esta política está Habilitada.

## Configurações de política do sistema de arquivos

### Configurações da política de exclusões

Esta seção descreve as configurações de política para configurar quais arquivos e diretórios no perfil de um usuário são excluídos do processo de sincronização.

#### LISTA DE EXCLUSÃO - ARQUIVOS

Lista de arquivos que são ignorados durante a sincronização. Os nomes dos arquivos devem ser caminhos relativos ao perfil do usuário (%USERPROFILE%). curingas são suportados em nomes de arquivos e em nomes de pastas, mas apenas curingas em nomes de arquivos são aplicados recursivamente.

Exemplos:

- `Desktop\Desktop.ini` ignora o arquivo `Desktop.ini` na pasta `Desktop`
- `%USERPROFILE%*.tmp` ignora todos os arquivos com a extensão `.tmp` em todo o perfil
- `AppData\Roaming\MyApp*.tmp` ignora todos os arquivos com a extensão `.tmp` em uma parte do perfil
- `Downloads*\a.txt` ignora `a.txt` em qualquer subpasta imediata da pasta `Downloads`.

Se esta política estiver desabilitada, nenhum arquivo será excluído. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhum arquivo será excluído.

### HABILITAR LISTA DE EXCLUSÃO PADRÃO - DIRETÓRIOS

Lista padrão de diretórios ignorados durante a sincronização. Use esta política para especificar diretórios de exclusão de GPO sem ter que preenchê-los manualmente.

Se você desabilitar esta política, o Profile Management não excluirá nenhum diretório por padrão.

Se você não configurar esta política aqui, o Profile Management usará o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não excluirá nenhum diretório por padrão.

### LISTA DE EXCLUSÃO - DIRETÓRIOS

Lista de pastas que são ignoradas durante a sincronização. Os nomes das pastas devem ser especificados como caminhos relativos ao perfil do usuário (%USERPROFILE%). curingas em nomes de pastas são suportados, mas não são aplicados recursivamente.

Exemplo:

- `Desktop` ignora a pasta `Desktop` no perfil do usuário

Se esta política estiver desativada, nenhuma pasta será excluída. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será excluída.

### VERIFICAÇÃO DE EXCLUSÃO DE LOGON

Esta configuração define o que o Profile Management faz se um perfil no armazenamento do usuário contiver arquivos ou pastas excluídos. As possíveis configurações de política e as ações correspondentes estão listadas na tabela a seguir:

| CONFIGURAÇÃO DA POLÍTICA | AÇÃO |
|---|---|
| A configuração está desativada ou o valor de "Sincronizar arquivos ou pastas excluídos no logon" está definido como padrão | O Profile Management sincroniza arquivos ou pastas excluídos do armazenamento do usuário para o perfil local quando um usuário faz logon. |
| A configuração está definida como "Ignorar arquivos ou pastas excluídos no logon" | O Profile Management ignora os arquivos ou pastas excluídos no armazenamento do usuário quando um usuário faz logon. |

| CONFIGURAÇÃO DA POLÍTICA | AÇÃO |
| --- | --- |
| A configuração está definida como "Excluir arquivos ou pastas excluídos no logon" | O Profile Management exclui os arquivos ou pastas excluídos no armazenamento do usuário quando um usuário faz logon. |
| A configuração não está definida no Web Studio | O valor do arquivo .ini é usado |
| A configuração não está definida no Web Studio ou no arquivo .ini | Os arquivos ou pastas excluídos são sincronizados do armazenamento do usuário para um perfil local quando um usuário faz logon. |

### MANIPULAÇÃO DE ARQUIVOS GRANDES - ARQUIVOS A SEREM CRIADOS COMO LINKS SIMBÓLICOS

Para melhorar o desempenho de logon e processar arquivos grandes, o Profile Management cria um link simbólico em vez de copiar os arquivos desta lista.

Você pode usar curingas em políticas que se referem a arquivos; por exemplo, `!ctx_localappdata!\Microsoft\Outlook*.OST`.

Para processar o arquivo de pasta offline (`*.ost`) do Microsoft Outlook, certifique-se de que a pasta **Outlook** não esteja excluída para o Profile Management.

Esses arquivos não podem ser acessados em várias sessões simultaneamente.

#### Configurações da política de sincronização

A seção **Sincronização** descreve as configurações de política para especificar quais arquivos e pastas em um perfil de usuário são sincronizados entre o sistema onde o perfil está instalado e o armazenamento de usuário.

### DIRETÓRIOS PARA SINCRONIZAR

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema onde está instalado e o armazenamento de usuário. Se você excluir uma pasta da sincronização, esta política permite incluir as subpastas da pasta excluída de volta à sincronização.

Os caminhos nesta lista devem ser relativos ao perfil do usuário. Curingas em nomes de pastas são suportados, mas não são aplicados recursivamente.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, apenas as pastas não excluídas no perfil do usuário serão sincronizadas.

### ARQUIVOS PARA SINCRONIZAR

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema onde está instalado e o armazenamento de usuário. Se você excluir uma pasta da sincronização, esta política permite incluir os arquivos dentro da pasta excluída de volta à sincronização.

Os caminhos nesta lista devem ser relativos ao perfil do usuário. Curingas são suportados em nomes de arquivos e em nomes de pastas, mas apenas curingas em nomes de arquivos são aplicados recursivamente. Curingas não podem ser aninhados.

Exemplos:

- `AppData\Local\Microsoft\Office\Access.qat` especifica um arquivo abaixo de uma pasta que é excluída na configuração padrão
- `AppData\Local\MyApp*.cfg` especifica todos os arquivos com a extensão `.cfg` na pasta de perfil `AppData\Local\MyApp` e suas subpastas

Desabilitar esta política tem o mesmo efeito que habilitá-la e configurar uma lista vazia.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, apenas os arquivos não excluídos no perfil do usuário serão sincronizados.

### PASTAS PARA ESPELHAR

Esta política permite resolver problemas envolvendo qualquer pasta transacional (também conhecida como pasta referencial). Essa pasta contém arquivos interdependentes, onde um arquivo faz referência ao outro.

Espelhar pastas permite que o Profile Management processe uma pasta transacional e seu conteúdo como uma única entidade, evitando o inchaço do perfil. Por exemplo, você pode espelhar a pasta **cookies do Internet Explorer** para que o Index.dat seja sincronizado com os cookies que ele indexa. Nessas situações, "a última gravação vence". Assim, arquivos em pastas espelhadas que foram modificados em mais de uma sessão são sobrescritos pela última atualização, resultando na perda de alterações do perfil.

Por exemplo, a tabela a seguir descreve como o Index.dat referencia cookies enquanto um usuário navega na Internet:

| CENÁRIO | COMO O INDEX.DAT REFERENCIA COOKIES | |
|---|---|---|
| Um usuário tem duas sessões do Internet Explorer, cada uma em um servidor diferente, e eles visitam sites diferentes em cada sessão. | Cookies de cada site são adicionados ao servidor apropriado. | Cookies de cada site são adicionados ao servidor apropriado. |
| O usuário faz logoff da primeira sessão ou no meio de uma sessão (se o recurso de gravação ativa estiver configurado) | Os cookies da segunda sessão devem substituir os cookies da primeira sessão. | |
| A primeira e a segunda sessões são mescladas e as referências aos cookies no Index.dat ficam desatualizadas | Navegações futuras em novas sessões resultam em mesclagem repetida e uma pasta de cookies inchada | |

Espelhar a pasta de cookies resolve o problema. Nesse caso, os cookies são sobrescritos pelos cookies da última sessão cada vez que o usuário faz logoff. Assim, o Index.dat permanece atualizado.

Se esta política não estiver configurada aqui, o valor do arquivo .ini é usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta é espelhada.

#### ACELERAR O ESPELHAMENTO DE PASTAS

Com esta política e a política **Pastas a espelhar** habilitadas, o **Profile Management armazena pastas espelhadas** em um disco virtual baseado em VHDX. Ele anexa o disco virtual durante os logons e o desanexa durante os logoffs. Habilitar esta política elimina a necessidade de copiar as pastas entre o armazenamento do usuário e os perfis locais e acelera o espelhamento de pastas.

### Configurações da política de desduplicação de arquivos

Arquivos idênticos podem existir entre vários perfis de usuário no armazenamento de usuário. Ter instâncias duplicadas de arquivos armazenados no armazenamento de usuário aumenta seu custo de armazenamento.

As políticas de desduplicação de arquivos permitem que o Profile Management remova arquivos duplicados do armazenamento de usuário e armazene uma instância deles em um local central

(chamado *armazenamento compartilhado*). Isso evita duplicações de arquivos no armazenamento de usuário, economizando assim seu custo de armazenamento.

#### Arquivos a serem incluídos no armazenamento compartilhado para desduplicação

Permite habilitar a desduplicação de arquivos e especificar arquivos a serem incluídos no armazenamento compartilhado para desduplicação.

#### Arquivos a serem excluídos do armazenamento compartilhado

Permite especificar arquivos a serem excluídos do armazenamento compartilhado. Use esta política juntamente com a política *Arquivos a serem incluídos no armazenamento compartilhado para desduplicação*.

#### Tamanho mínimo dos arquivos a serem desduplicados dos contêineres de perfil

Permite especificar o tamanho mínimo dos arquivos a serem desduplicados dos contêineres de perfil. O tamanho deve ser de 256 MB ou superior.

Precedência de configuração:

1. Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.
2. Se esta configuração não for definida aqui nem no arquivo .ini, o valor será 256.

### Configurações de política de redirecionamento de pasta

Esta seção contém configurações de política que especificam se as pastas que aparecem com frequência em perfis devem ser redirecionadas para um local de rede compartilhado.

#### Conceder acesso de administrador

Esta configuração permite que um administrador acesse o conteúdo das pastas redirecionadas de um usuário.

> **Observação:**
>
> Esta configuração concede permissões a administradores que têm acesso completo e irrestrito ao domínio.
>
> Por padrão, esta configuração está desabilitada e os usuários recebem acesso exclusivo ao conteúdo de suas pastas redirecionadas.

### Incluir nome de domínio

Esta configuração permite a inclusão da variável de ambiente `%userdomain%` como parte do caminho UNC. Este caminho UNC é especificado para pastas redirecionadas.

Por padrão, esta configuração está desabilitada. E a variável de ambiente `%userdomain%` não é incluída como parte do caminho UNC que é especificado para pastas redirecionadas.

### Configurações de política do AppData(Roaming)

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **AppData(Roaming)** para um local de rede compartilhado.

#### CAMINHO DO APPDATA(ROAMING)

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **AppData(Roaming)** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

#### CONFIGURAÇÕES DE REDIRECIONAMENTO PARA APPDATA(ROAMING)

Esta configuração especifica como redirecionar o conteúdo da pasta **AppData(Roaming)**.

Por padrão, o conteúdo é redirecionado para um caminho UNC. Para obter mais informações, consulte a seção Caminho para o armazenamento do usuário.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

### Configurações de política de Contatos

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Contatos** para um local de rede compartilhado.

#### CAMINHO DE CONTATOS

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **Contatos** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

#### CONFIGURAÇÕES DE REDIRECIONAMENTO PARA CONTATOS

Esta configuração especifica como redirecionar o conteúdo da pasta **Contatos**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

### Configurações de política de Downloads

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Downloads** para um local de rede compartilhado.

#### CAMINHO DE DOWNLOADS

Esta configuração especifica o local de rede para o qual os arquivos na pasta **Downloads** são redirecionados.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

#### CONFIGURAÇÕES DE REDIRECIONAMENTO PARA DOWNLOADS

Esta configuração especifica como redirecionar o conteúdo da pasta **Downloads**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

### Configurações de política de Links

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Links** para um local de rede compartilhado.

#### CAMINHO DOS LINKS

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **Links** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for definida aqui, o Profile Management não redireciona a pasta especificada.

#### CONFIGURAÇÕES DE REDIRECIONAMENTO PARA LINKS

Esta configuração especifica como redirecionar o conteúdo da pasta **Links**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Se esta configuração não for definida aqui, o Profile Management não redireciona a pasta especificada.

### Configurações de política de Pesquisas

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Pesquisas** para um local de rede compartilhado.

#### CONFIGURAÇÕES DE REDIRECIONAMENTO PARA PESQUISAS

Esta configuração especifica como redirecionar o conteúdo da pasta **Pesquisas**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Se esta configuração não for definida aqui, o Profile Management não redireciona a pasta especificada.

#### CAMINHO DE PESQUISAS

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **Pesquisas** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for definida aqui, o Profile Management não redireciona a pasta especificada.

## Configurações de política de log

Esta seção contém configurações de política que configuram o registro do Profile Management.

### Ações do Active Directory

Esta configuração habilita ou desabilita o registro detalhado das ações realizadas no Active Directory.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida no Web Studio, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

**Informações comuns**

Esta configuração habilita ou desabilita o registro detalhado de informações comuns.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte é registrado:

- Erros
- Informações gerais

**Avisos comuns**

Esta configuração habilita ou desabilita o registro detalhado de avisos comuns.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte é registrado:

- Erros
- Informações gerais

**Habilitar registro**

Esta configuração habilita ou desabilita o registro do Profile Management no modo de depuração (registro detalhado). No modo de depuração, informações de status extensas são registradas nos arquivos de log localizados em "%SystemRoot%\System32\Logfiles\UserProfileManager".

Por padrão, esta configuração está desabilitada e apenas erros são registrados.

A Citrix® recomenda habilitar esta configuração apenas se você estiver solucionando problemas do Profile Management.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, somente os erros serão registrados.

**Ações do sistema de arquivos**

Esta configuração habilita ou desabilita o registro detalhado das ações realizadas no sistema de arquivos.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

**Notificações do sistema de arquivos**

Esta configuração habilita ou desabilita o registro detalhado das notificações do sistema de arquivos.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

### Logoff

Esta configuração habilita ou desabilita o registro detalhado de logoffs de usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não estiver configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

### Logon

Esta configuração habilita ou desabilita o registro detalhado de logons de usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

### Tamanho máximo do arquivo de log

Esta configuração especifica o tamanho máximo permitido para o arquivo de log do Profile Management, em bytes.

Por padrão, este valor é definido como 1048576 bytes (1 MB).

A Citrix recomenda aumentar o tamanho deste arquivo para 5 MB ou mais, se você tiver espaço em disco suficiente. Se o arquivo de log exceder o tamanho máximo:

- Um backup existente do arquivo (.bak) é excluído
- O arquivo de log é renomeado para .bak

- Um novo arquivo de log é criado

O arquivo de log é criado em `%SystemRoot%\System32\Logfiles\UserProfileManager`.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, o valor padrão será usado.

**Caminho para o arquivo de log**

Esta configuração especifica um caminho alternativo para salvar o arquivo de log do Profile Management.

Por padrão, esta configuração está desabilitada e os arquivos de log são salvos no local padrão: %SystemRoot%\System32\Logfiles\UserProfileManager.

O caminho pode apontar para uma unidade local ou uma unidade de rede remota (caminho UNC). Caminhos remotos podem ser úteis em grandes ambientes distribuídos, mas podem criar um tráfego de rede significativo, o que pode ser inadequado para arquivos de log. Para máquinas virtuais provisionadas com um disco rígido persistente, defina um caminho local para essa unidade. Essa configuração garante que os arquivos de log sejam preservados quando a máquina for reiniciada. Para máquinas virtuais sem um disco rígido persistente, definir um caminho UNC permite reter os arquivos de log. No entanto, a conta do sistema para as máquinas deve ter acesso de gravação ao compartilhamento UNC. Use um caminho local para quaisquer laptops gerenciados pelo recurso de perfis offline.

Se um caminho UNC for usado para arquivos de log, a Citrix recomenda que uma lista de controle de acesso apropriada seja aplicada à pasta do arquivo de log. Essa configuração garante que apenas contas de usuário ou computador autorizadas possam acessar os arquivos armazenados.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, o local padrão %SystemRoot%\System32\Logfiles\UserProfileManager será usado.

**Informações personalizadas do usuário**

Esta configuração habilita ou desabilita o registro detalhado de informações personalizadas do usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

**Valores da política no logon e logoff**

Esta configuração ativa ou desativa o registro detalhado dos valores da política quando um usuário faz logon e logoff.

Por padrão, esta configuração está desativada.

Ao ativar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja ativada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

**Ações do Registro**

Esta configuração ativa ou desativa o registro detalhado das ações realizadas no Registro.

Por padrão, esta configuração está desativada.

Ao ativar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja ativada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

### Diferenças de registro no logoff

Essa configuração habilita ou desabilita o registro detalhado de quaisquer diferenças no registro quando um usuário faz logoff.

Por padrão, essa configuração está desabilitada.

Ao habilitar essa configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se essa configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se essa configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

## Configurações de política de tratamento de perfil

Esta seção inclui configurações de política que especificam como o Profile Management lida com perfis de usuário.

### Atraso antes de excluir perfis em cache

Esta configuração especifica uma extensão opcional ao atraso, em minutos, antes que o Profile Management exclua perfis armazenados em cache localmente no logoff.

Um valor de 0 exclui os perfis imediatamente ao final do processo de logoff. O Profile Management verifica os logoffs a cada minuto. Como resultado, um valor de 60 garante que os perfis sejam excluídos entre um e dois minutos após os usuários fazerem logoff. Esta ação depende de quando a última verificação ocorreu. Estender o atraso é útil se você souber que um processo mantém arquivos ou o hive do registro do usuário abertos durante o logoff. Com perfis grandes, este processo também pode acelerar o logoff.

Por padrão, este valor é definido como 0 e o Profile Management exclui os perfis armazenados em cache localmente imediatamente.

Ao habilitar esta configuração, certifique-se de que a opção Excluir perfis armazenados em cache localmente no logoff também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, os perfis serão excluídos imediatamente.

### Excluir perfis armazenados em cache localmente no logoff

Esta configuração especifica se os perfis armazenados em cache localmente são excluídos depois que um usuário faz logoff.

Quando esta configuração está habilitada, o cache de perfil local de um usuário é excluído depois que ele faz logoff. A Citrix® recomenda habilitar esta configuração para servidores de terminal.

Por padrão, esta configuração está desabilitada e o cache de perfil local de um usuário é retido depois que ele faz logoff.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, os perfis em cache não serão excluídos.

### Tratamento de conflitos de perfil local

Essa configuração define como o Profile Management se comporta se um perfil de usuário existir em ambos os seguintes locais:

- Repositório de usuário
- Perfil de usuário local do Windows (não é um perfil de usuário Citrix)

Por padrão, o Profile Management usa o perfil local do Windows, mas não o altera de forma alguma.

Para controlar como o Profile Management se comporta, escolha uma das seguintes opções:

- Usar perfil local. O Profile Management usa o perfil local, mas não o altera de forma alguma.
- Excluir perfil local. O Profile Management exclui o perfil de usuário local do Windows e, em seguida, importa o perfil de usuário Citrix do repositório de usuário.
- Renomear perfil local. O Profile Management renomeia o perfil de usuário local do Windows (para fins de backup) e, em seguida, importa o perfil de usuário Citrix do repositório de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, os perfis locais existentes serão usados.

### Migração de perfis existentes

Essa configuração especifica os tipos de perfil migrados para o repositório de usuário durante o logon se um usuário não tiver um perfil atual no repositório de usuário.

O Profile Management pode migrar perfis existentes "em tempo real" durante o logon, se um usuário não tiver um perfil no repositório de usuário. Depois disso, o perfil do repositório de usuário é usado pelo Profile Management em ambos os seguintes casos:

- Sessão atual
- Qualquer outra sessão configurada com o caminho para o mesmo armazenamento de usuário

Por padrão, tanto os perfis locais quanto os perfis móveis são migrados para o armazenamento de usuário durante o logon.

Para especificar os tipos de perfil migrados para o armazenamento de usuário durante o logon, escolha uma das seguintes opções:

- Perfis locais e móveis
- Local
- Móvel
- Nenhum (Desabilitado)

Se você selecionar **Nenhum**, o sistema usa o mecanismo existente do Windows para criar perfis, como se estivesse em um ambiente onde o Profile Management não está instalado.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, os perfis locais e móveis existentes serão migrados.

### Migração automática de perfis de aplicativos existentes

Esta configuração habilita ou desabilita a migração automática de perfis de aplicativos existentes entre diferentes sistemas operacionais. Os perfis de aplicativos incluem tanto os dados do aplicativo na pasta `AppData` quanto as entradas de registro em `HKEY_CURRENT_USER\SOFTWARE`. Esta configuração pode ser útil em casos onde você deseja migrar seus perfis de aplicativos entre diferentes sistemas operacionais.

Por exemplo, suponha que você atualize seu sistema operacional (SO) do Windows 10 versão 1803 para o Windows 10 versão 1809. Se esta configuração estiver habilitada, o Profile Management migra automaticamente as configurações de aplicativo existentes para o Windows

10 versão 1809 na primeira vez que cada usuário faz logon. Como resultado, os dados do aplicativo na pasta `AppData` e as entradas de registro em HKEY_CURRENT_USER\SOFTWARE são migrados.

Se houver vários perfis de aplicativos existentes, o Profile Management executa a migração na seguinte ordem de prioridade:

1. Perfis do mesmo tipo de SO (SO de sessão única para SO de sessão única e SO de múltiplas sessões para SO de múltiplas sessões).
2. Perfis da mesma família de SO Windows; por exemplo, Windows 10 para Windows 10, ou Windows Server 2016 para Windows Server 2016).
3. Perfis de uma versão anterior do SO; por exemplo, Windows 7 para Windows 10, ou Windows Server 2012 para Windows 2016.
4. Perfis do SO mais próximo.

**Nota:** Você deve especificar o nome abreviado do SO incluindo a variável "!CTX_OSNAME!" no caminho do armazenamento do usuário. Isso permite que o Profile Management localize os perfis de aplicativo existentes.

Se essa configuração não for configurada aqui, a configuração do arquivo .ini será usada.

Se essa configuração não for configurada aqui ou no arquivo .ini, ela será desabilitada por padrão.

### Caminho para o perfil de modelo

Essa configuração especifica o caminho para o perfil que você deseja que o Profile Management use como modelo para criar perfis de usuário.

O caminho especificado deve ser o caminho completo para a pasta que contém o arquivo de registro NTUSER.DAT e quaisquer outras pastas e arquivos necessários para o perfil de modelo.

Nota: Não inclua NTUSER.DAT no caminho. Por exemplo, com o arquivo `\\myservername\myprofiles\template\ntuser.dat`, defina o local como `\\myservername\myprofiles\template`.

Use caminhos absolutos, que podem ser caminhos UNC ou caminhos na máquina local. Use este último, por exemplo, para especificar um perfil de modelo permanentemente em uma imagem do Citrix Provisioning™ Services. Caminhos relativos não são suportados.

Nota: Essa configuração não oferece suporte à expansão de atributos do Active Directory, variáveis de ambiente do sistema ou as variáveis `%USERNAME%` e `%USERDOMAIN%`.

Por padrão, essa configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se essa configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se essa configuração não for configurada aqui ou no arquivo .ini, nenhum modelo será usado.

**Perfil de modelo substitui perfil local**

Essa configuração permite que o perfil de modelo substitua o perfil local ao criar perfis de usuário.

Considere que um usuário não tem um perfil de usuário Citrix, mas tem um perfil de usuário local do Windows. Nesse caso, por padrão, o perfil local é usado e migrado para o armazenamento de usuário, se esse valor estiver habilitado. Habilitar essa configuração de política permite que o perfil de modelo substitua o perfil local usado ao criar perfis de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

**Perfil de modelo substitui perfil móvel**

Essa configuração permite que o perfil de modelo substitua um perfil móvel ao criar perfis de usuário.

Considere que um usuário não tem um perfil de usuário Citrix, mas tem um perfil de usuário móvel do Windows. Nesse caso, por padrão, o perfil móvel é usado e migrado para o armazenamento de usuário, se esse valor estiver habilitado. Habilitar essa configuração de política permite que o perfil de modelo substitua o perfil móvel usado ao criar perfis de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

**Perfil de modelo usado como um perfil obrigatório do Citrix para todos os logons**

Essa configuração permite que o Profile Management use o perfil de modelo como o perfil padrão para criar todos os perfis de usuário.

Por padrão, essa configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

## Configurações da política de contêiner de perfil

### Contêiner de perfil

Pastas grandes associadas a um perfil de usuário resultam em um logon lento. O Citrix Profile Management fornece uma solução de perfil baseada em VHDX que permite especificar as pastas a serem contidas no disco de perfil (arquivos VHDX). Esta solução reduz os tempos de logon mapeando as pastas especificadas para o disco de perfil que é armazenado na rede. O contêiner de perfil anexa o disco de perfil contendo essas pastas durante o logon, eliminando assim a necessidade de salvar uma cópia das pastas no perfil local. Isso diminui os tempos de logon.

### Habilitar cache local para contêineres de perfil

Esta política habilita o suporte a cache local para contêineres de perfil do Citrix Profile Management. Com a política definida como **Habilitado**, cada perfil local serve como um cache local de seu contêiner de perfil do Citrix Profile Management. Se o streaming de perfil estiver em uso, os arquivos armazenados em cache localmente são criados sob demanda. Caso contrário, eles são criados durante os logons do usuário. Para usar o recurso de cache local, coloque um perfil de usuário inteiro em seu contêiner de perfil do Citrix Profile Management.

### Pastas a serem excluídas do contêiner de perfil

Lista de pastas a serem excluídas de um contêiner de perfil do Citrix Profile Management.

### Pastas a serem incluídas no contêiner de perfil

Lista de pastas a serem mantidas em um contêiner de perfil do Citrix Profile Management quando suas pastas pai são excluídas.

As pastas nesta lista devem ser subpastas das pastas excluídas. Caso contrário, esta configuração não funciona.

### Arquivos a serem incluídos no contêiner de perfil

Lista de arquivos a serem incluídos em um contêiner de perfil do Citrix Profile Management.

Os arquivos nesta lista devem estar dentro das pastas excluídas. Caso contrário, esta configuração não funciona.

### Arquivos a serem excluídos do contêiner de perfil

Lista de arquivos a serem excluídos de um contêiner de perfil do Citrix Profile Management.

### Habilitar compactação de disco VHD

Permite habilitar a compactação de disco VHD para o Gerenciamento de Perfis. Se ativado, os discos VHD são compactados automaticamente no logoff do usuário quando certas condições são atendidas. Esta política permite economizar o espaço de armazenamento consumido pelo contêiner de perfil, contêiner do OneDrive e contêiner de pasta espelhada.

Dependendo das suas necessidades e dos recursos disponíveis, você pode ajustar as configurações e o comportamento padrão de compactação de VHD usando as políticas **Taxa de espaço livre para acionar a compactação de disco VHD**, **Número de logoffs para acionar a compactação de disco VHD** e **Desabilitar desfragmentação para compactação de disco VHD** em Configurações avançadas.

### Habilitar autoexpansão de VHD para contêiner de perfil

Permite especificar se a autoexpansão de VHD deve ser habilitada para o contêiner de perfil. Quando habilitada, todas as configurações de autoexpansão de VHD se aplicam ao contêiner de perfil.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui ou no arquivo .ini, ela será desabilitada.

### Habilitar acesso exclusivo a contêineres VHD

Por padrão, os contêineres VHD permitem acesso concorrente. Com esta configuração habilitada, eles permitem apenas um acesso por vez. Este recurso se aplica a contêineres de perfil e contêineres do OneDrive.

> **Observação:**
>
> Habilitar esta configuração para contêineres de perfil em uma solução de perfil baseada em contêiner desabilita automaticamente a configuração *Habilitar gravação de várias sessões para contêineres de perfil*.
>
> Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, a configuração será desabilitada.

### Fazer logoff de usuários quando o contêiner de perfil não estiver disponível durante o logon

Permite forçar o logoff de usuários quando o contêiner de perfil não estiver disponível durante o logon do usuário e (opcionalmente) personalizar a mensagem de erro que os usuários veem.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, a configuração será desativada.

### Usuários e grupos para acessar o contêiner de perfil

Permite especificar quais usuários e grupos de domínio AD têm permissão `Read & Execute` em contêineres de perfil. Por padrão, um contêiner de perfil é acessível apenas ao seu proprietário.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, a configuração do arquivo .ini será usada.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, o contêiner de perfil será acessível apenas ao seu proprietário.

## Configurações de política de registro

Esta seção contém configurações de política que especificam quais chaves de registro são incluídas ou excluídas do processamento do Profile Management.

### Lista de exclusão

Lista de chaves de registro no hive HKCU que são ignoradas durante o logoff.

Exemplo: Software\Policies

Se esta política estiver desabilitada, nenhuma chave de registro será excluída. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma chave de registro será excluída.

### Lista de inclusão

Lista de chaves de registro no hive HKCU que são processadas durante o logoff.

Exemplo: Software\Adobe.

Se esta política estiver habilitada, apenas as chaves desta lista serão processadas. Se esta política estiver desabilitada, o hive HKCU completo será processado. Se esta política não estiver

configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, todo o HKCU será processado.

#### Habilitar Lista de Exclusão Padrão - Profile Management 5.5

Lista padrão de chaves de registro no hive HKCU que não são sincronizadas com o perfil do usuário. Use esta política para especificar arquivos de exclusão de GPO sem precisar preenchê-los manualmente.

Se você desabilitar esta política, o Profile Management não excluirá nenhuma chave de registro por padrão. Se você não configurar esta política aqui, o Profile Management usará o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não excluirá nenhuma chave de registro por padrão.

#### Backup do NTUSER.DAT

Habilita um backup da última cópia boa conhecida de NTUSER.DAT e o rollback em caso de corrupção.

Se você não configurar esta política aqui, o Profile Management usa o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não faz backup do NTUSER.DAT.

### Configurações de política de perfis de usuário transmitidos

Esta seção contém configurações de política que especificam como o Profile Management processa perfis de usuário transmitidos.

#### Sempre armazenar em cache

Esta configuração especifica se o Profile Management armazena em cache arquivos transmitidos o mais rápido possível após o logon de um usuário. O armazenamento em cache de arquivos após o logon de um usuário economiza largura de banda da rede, melhorando a experiência do usuário.

Use esta configuração com a configuração de **Streaming de perfil**.

Por padrão, esta configuração está desabilitada e os arquivos transmitidos não são armazenados em cache o mais rápido possível após o logon de um usuário.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada nem aqui nem no arquivo .ini, ela será desabilitada.

### Tamanho do cache sempre

Esta configuração especifica um limite inferior, em MB, para o tamanho dos arquivos que são transmitidos. O Profile Management armazena em cache quaisquer arquivos deste tamanho ou maiores o mais rápido possível após o logon de um usuário.

Por padrão, o valor é definido como 0 (zero) e o recurso de cache de perfil completo é usado. Quando o recurso de cache de perfil completo está habilitado, o Profile Management busca todo o conteúdo do perfil no armazenamento do usuário, após o logon de um usuário, como uma tarefa em segundo plano.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada nem aqui nem no arquivo .ini, ela será desabilitada.

### Streaming de perfil

Esta configuração habilita e desabilita o recurso de perfis de usuário transmitidos do Citrix®. Quando habilitado, os arquivos e pastas de perfil são buscados do armazenamento do usuário para o computador local somente quando os usuários os acessam após o logon. As entradas de registro e os arquivos na área pendente são buscados imediatamente.

Por padrão, o streaming de perfil está desativado.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida nem aqui nem no arquivo .ini, ela será desativada.

### Ativar exclusão de streaming de perfil

Esta configuração especifica quais perfis de usuário dentro de uma OU são transmitidos, com base nos grupos de usuários do Windows.

Quando ativado, apenas os perfis de usuário dentro dos grupos de usuários especificados são transmitidos. Todos os outros perfis de usuário são processados normalmente.

Por padrão, esta configuração está desativada e todos os perfis de usuário dentro de uma OU são processados normalmente.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida nem aqui nem no arquivo .ini, todos os perfis de usuário serão processados.

### Ativar exclusão de streaming de perfil

Quando a exclusão de streaming de perfil está ativada:

- O Profile Management não transmite pastas na lista de exclusão
- Todas as pastas são buscadas imediatamente do armazenamento do usuário para o computador local quando um usuário faz logon

Para obter mais informações, consulte Transmitir perfis de usuário.

### Tempo limite para arquivos de bloqueio de área pendente

Esta configuração especifica o número de dias após os quais os arquivos dos usuários são gravados de volta no armazenamento de usuário da área pendente, se o armazenamento de usuário permanecer bloqueado quando seu servidor de armazenamento ficar sem resposta. Esse comportamento evita o inchaço na área pendente e garante que o armazenamento de usuário sempre contenha os arquivos mais atualizados.

Por padrão, esta configuração é definida como 1 (um) dia.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada nem aqui nem no arquivo .ini, o valor padrão será usado.

### HABILITAR STREAMING DE PERFIL PARA ÁREA PENDENTE

Permite habilitar o recurso de streaming de perfil para arquivos e pastas na área pendente.

A área pendente é usada para garantir a consistência do perfil enquanto o streaming de perfil está habilitado. Ela armazena temporariamente arquivos e pastas de perfil alterados em sessões simultâneas.

Por padrão, esta política está desabilitada, e todos os arquivos e pastas na área pendente são buscados para o perfil local no logon. Com esta política habilitada, os arquivos na área pendente são buscados para o perfil local somente quando solicitados. Use a política com a política de streaming de perfil para garantir uma experiência de logon ideal em cenários de sessão simultânea.

A política se aplica a pastas na área pendente quando a política Habilitar streaming de perfil para pastas está habilitada.

## Configurações de política da camada de personalização do usuário

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- O tamanho máximo que qualquer novo disco de camada de usuário pode atingir.

Para fazer isso, estas duas políticas aparecem na lista de políticas disponíveis:

- Caminho do Repositório da Camada de Usuário - Insira um caminho no formato '\\nome ou endereço do servidor\nome da pasta' no campo Valor.
- Tamanho da Camada de Usuário em GB - O tamanho padrão da camada de usuário de 10 GB é o mínimo que a Citrix® recomenda. Uma camada de usuário é um disco de provisionamento dinâmico que se expande até o tamanho definido à medida que o espaço é usado. As camadas de usuário nunca diminuem de tamanho.

> **Nota:**
>
> Aumentar o Tamanho da Camada de Usuário afeta novas camadas de usuário e expande as existentes. Diminuir o tamanho da camada afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

> Para obter mais informações, consulte Camada de personalização do usuário.

## Configurações de política do Virtual Delivery Agent

A seção Virtual Delivery Agent (VDA) contém configurações de política que controlam a comunicação entre o VDA e os controladores de um site.

Importante: O VDA requer informações fornecidas por essas configurações para se registrar em um Delivery Controller™, se você não estiver usando o recurso de atualização automática. Como essas informações são necessárias para o registro, você deve configurar as seguintes configurações usando o Editor de Política de Grupo, a menos que você forneça essas informações durante a instalação do VDA:

- Máscara de rede IPv6 de registro do Controller
- Porta de registro do Controller
- SIDs do Controller

- Controladores
- Usar apenas registro de controlador IPv6
- GUID do Site

### Máscara de rede IPv6 de registro do Controller

Esta configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial (em vez de um IP global, se um estiver registrado). Esta configuração especifica o endereço IPv6 e a rede onde o VDA se registra. O VDA se registra apenas no primeiro endereço que corresponde à máscara de rede especificada. Esta configuração é válida apenas se a configuração de política Usar apenas registro de controlador IPv6 estiver ativada.

Por padrão, esta configuração está em branco.

### Porta de registro do Controller

Use esta configuração apenas se a configuração **Habilitar atualização automática de controladores** estiver desabilitada.

Esta configuração especifica o número da porta TCP/IP que o VDA usa para se registrar em um Controller ao usar o registro baseado em registro.

Por padrão, o número da porta é definido como 80.

### SIDs do Controller

Use esta configuração somente se a configuração **Habilitar atualização automática de controllers** estiver desabilitada.

Esta configuração especifica uma lista de identificadores de segurança (SIDs) de controller separados por espaço que o VDA usa para se registrar em um Controller ao usar o registro baseado em registro. Esta configuração é opcional e pode ser usada com a configuração **Controllers** para restringir a lista de Controllers usados para registro.

Por padrão, esta configuração está em branco.

### Controladores

Use esta configuração somente se a configuração **Habilitar atualização automática de controllers** estiver desabilitada.

Esta configuração especifica uma lista de Nomes de Domínio Totalmente Qualificados (FQDNs) de controller separados por espaço que o VDA usa para se registrar em um Controller ao usar o

registro baseado em registro. Esta configuração é opcional e pode ser usada com a configuração **SIDs do Controller**.

Por padrão, esta configuração está em branco.

### Habilitar atualização automática de controladores

Esta configuração permite que o VDA se registre em um Controller automaticamente após a instalação.

Depois que o VDA se registra, o Controller com o qual ele se registrou envia uma lista dos FQDNs e SIDs atuais do controller para o VDA. O VDA grava esta lista no armazenamento persistente. Cada Controller também verifica o banco de dados do Site a cada 90 minutos para obter informações do Controller. O Controller envia listas atualizadas para seus VDAs registrados se um dos seguintes ocorrer:

- Um Controller foi adicionado ou removido desde a última verificação
- Uma alteração de política ocorreu

O VDA aceita conexões de todos os Controllers na lista mais recente que recebeu.

Por padrão, esta configuração está ativada.

### Usar apenas o registro do controlador IPv6

Esta configuração controla qual forma de endereço o VDA usa para se registrar no Controller:

- Quando ativado, o VDA se registra no Controller usando o endereço IPv6 da máquina. Quando o VDA se comunica com o Controller, ele usa a seguinte ordem de endereços: endereço IP global, Endereço Local Único (ULA), endereço link-local (se nenhum outro endereço IPv6 estiver disponível).
- Quando desativado, o VDA se registra e se comunica com o Controller usando o endereço IPv4 da máquina.

Por padrão, esta configuração está desativada.

### GUID do Site

Use esta configuração somente se a configuração **Ativar atualização automática de controladores** estiver desativada.

Esta configuração especifica o Identificador Globalmente Único (GUID) do site que o VDA usa para se registrar em um Controller ao usar o registro baseado no Active Directory.

Por padrão, esta configuração está em branco.

## Configurações de política do HDX™ 3D Pro

A seção HDX 3D Pro inclui configurações de política para habilitar e configurar a ferramenta de configuração de qualidade de imagem para usuários. Essa ferramenta permite que os usuários otimizem o uso da largura de banda disponível. Para essa otimização, o equilíbrio entre a qualidade da imagem e a capacidade de resposta é ajustado em tempo real.

### Habilitar sem perdas

Essa configuração especifica se os usuários podem habilitar e desabilitar a compactação sem perdas usando a ferramenta de configuração de qualidade de imagem. Por padrão, os usuários não têm a opção de habilitar a compactação sem perdas.

Considere que um usuário habilita a compressão sem perdas. Neste caso, a qualidade da imagem é automaticamente definida para o valor máximo disponível na ferramenta de configuração de imagem. Por padrão, a compressão baseada em GPU ou CPU pode ser usada, de acordo com as capacidades do dispositivo do usuário e do computador host.

### Configurações de qualidade do HDX 3D Pro

Essa configuração especifica os valores mínimo e máximo disponíveis para os usuários na ferramenta de configuração de qualidade de imagem. Usando esses valores, os usuários podem definir o intervalo de ajuste da qualidade da imagem na ferramenta de configuração de qualidade de imagem.

Especifique valores de qualidade de imagem entre 0 e 100, inclusive. O valor máximo deve ser maior ou igual ao valor mínimo.

## Configurações de política de monitoramento

A seção **Monitoramento** inclui configurações de política para monitoramento de processos, recursos e falhas de aplicativos.

O escopo dessas políticas pode ser definido com base no seguinte:

- Site
- Grupo de entrega
- Tipo de grupo de entrega
- Unidade organizacional
- Tags

### Políticas para monitoramento de processos e recursos

Cada ponto de dados para CPU, memória e processos é coletado do VDA e armazenado no banco de dados de Monitoramento. O envio dos pontos de dados do VDA consome largura de banda da rede e o armazenamento deles consome um espaço considerável no banco de dados de monitoramento. Considere que você não deseja monitorar dados de recursos ou dados de processos, ou ambos, para um escopo específico. Por exemplo, um grupo de entrega ou unidade organizacional específica. Neste caso, é recomendado desabilitar a política.

#### HABILITAR MONITORAMENTO DE PROCESSOS

Habilite esta configuração para permitir o monitoramento de processos em execução em máquinas com VDAs. Estatísticas como uso de CPU e memória são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificações em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Desabilitado.

#### HABILITAR MONITORAMENTO DE RECURSOS

Habilite esta configuração para permitir o monitoramento de contadores de desempenho críticos em máquinas com VDAs. Estatísticas (como uso de CPU e memória, IOPS e dados de latência de disco) são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificação em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Habilitado.

#### ESCALABILIDADE

Os dados de CPU e memória são enviados para o banco de dados de cada VDA em intervalos de 5 minutos. Os dados de processo (se ativados) são enviados para o banco de dados em intervalos de 10 minutos. Os dados de IOPS e latência de disco são enviados para o banco de dados em intervalos de 1 hora.

#### DADOS DE CPU E MEMÓRIA

Os dados de CPU e memória são **ativados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

| GRANULARIDADE DOS DADOS | NÚMERO DE DIAS |
|---|---|
| Dados de 5 Minutos | 1 Dia |
| Dados de 10 Minutos | 7 Dias |
| Dados Horários | 30 Dias |

| GRANULARIDADE DOS DADOS | NÚMERO DE DIAS |
|---|---|
| Dados Diários | 90 Dias |

### DADOS DE IOPS E LATÊNCIA DE DISCO

Os dados de IOPS e latência de disco são **Ativados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

| GRANULARIDADE DOS DADOS | NÚMERO DE DIAS |
|---|---|
| Dados por Hora | 3 Dias |
| Dados Diários | 90 Dias |

Com as configurações de retenção de dados, aproximadamente 276 KB de espaço em disco são necessários para armazenar o seguinte para um VDA durante um período de um ano:

- CPU
- Memória
- IOPS
- Dados de latência de disco

| NÚMERO DE MÁQUINAS | ARMAZENAMENTO APROXIMADO NECESSÁRIO |
|---|---|
| 1 | 276 KB |
| 1K | 270 MB |
| 40K | 10.6 GB |

### DADOS DO PROCESSO

Os dados do processo estão **Desativados** por padrão. Recomenda-se habilitar os dados do processo em um subconjunto de máquinas conforme a necessidade. As configurações padrão de retenção de dados para os dados do processo são as seguintes:

| GRANULARIDADE DOS DADOS | NÚMERO DE DIAS |
|---|---|
| Dados de 10 minutos | 1 Dia |

| GRANULARIDADE DOS DADOS | NÚMERO DE DIAS |
|---|---|
| Dados por Hora | 7 Dias |

Se os dados do processo forem habilitados com as configurações de retenção padrão, os dados do processo consumiriam aproximadamente 1,5 MB por VDA e 3 MB por VDA de Serviços de Terminal (TS VDA) durante um período de um ano.

| NÚMERO DE MÁQUINAS | ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA VDA | ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA TS VDA |
|---|---|---|
| 1 | 1.5 MB | 3 MB |
| 1K | 1.5 GB | 3 GB |

**Nota:**

Os números fornecidos anteriormente não incluem o espaço do Índice. E todos os cálculos são aproximados e variam dependendo da implantação.

#### CONFIGURAÇÕES OPCIONAIS

Você pode modificar as configurações de retenção padrão para atender às suas necessidades. No entanto, esta configuração consome armazenamento extra. Ao habilitar as configurações abaixo, você pode obter maior precisão nos dados de utilização do processo. As configurações que podem ser habilitadas são:

#### ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

#### ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

Essas configurações podem ser habilitadas a partir do cmdlet do PowerShell de Monitoramento: Set-MonitorConfiguration

### Políticas para monitoramento de falhas de aplicativos

A guia **Falha de Aplicativo**, por padrão, exibe apenas falhas de aplicativos de VDAs de SO de múltiplas sessões. As configurações de monitoramento de falhas de aplicativos podem ser modificadas com as seguintes políticas de Monitoramento:

### HABILITAR O MONITORAMENTO DE FALHAS DE APLICATIVOS

Use esta configuração para configurar o monitoramento de falhas de aplicativos para monitorar erros ou falhas de aplicativos (travamentos e exceções não tratadas), ou ambos. Desabilite o monitoramento de falhas de aplicativos definindo o **Valor** como **Nenhum**. O padrão para esta configuração é apenas falhas de aplicativos.

### HABILITAR O MONITORAMENTO DE FALHAS DE APLICATIVOS EM VDAS DE SO DE SESSÃO ÚNICA

Por padrão, apenas as falhas de aplicativos hospedados em VDAs de SO de múltiplas sessões são monitoradas. Para monitorar VDAs de SO de sessão única, defina a política como **Permitido**. O padrão para esta configuração é **Proibido**.

### LISTA DE APLICATIVOS EXCLUÍDOS DO MONITORAMENTO DE FALHAS

Especifique uma lista de aplicativos que não devem ser monitorados quanto a falhas. Por padrão, esta lista está vazia.

## Política para coleta de dados para Análise

### COLETA DE DADOS VDA PARA ANÁLISE

Use a política para habilitar ou desabilitar o serviço Monitor de coletar métricas relacionadas a desempenho e segurança dos VDAs para Análise de Desempenho e Segurança. Por padrão, a política é **Permitida**. Defina a política como **Proibida** para interromper a coleta de dados dos VDAs.

### COLETA DE METADADOS DE LOCAL DA ÁREA DE TRANSFERÊNCIA PARA MONITORAMENTO DE SEGURANÇA

Use a política para habilitar ou desabilitar a coleta de metadados de local da área de transferência pelo serviço Broker para monitoramento de segurança, auditoria e conformidade. Por padrão, a política é **Habilitada**. Defina a política como **Desabilitada** para interromper a coleta de dados dos VDAs.

### COLETA DE DADOS DE DIAGNÓSTICO PARA MONITORAMENTO DE DESEMPENHO

Use esta política para habilitar o serviço de monitoramento para coletar dados de diagnóstico, como informações de sessão, estados de serviço UPM/EUEM, otimização do Microsoft Teams e protocolos de conexão. Por padrão, a política é **Habilitada**. Defina a política como **Desabilitada** para interromper a coleta de dados dos VDAs.

### Dicas de planejamento de armazenamento

**Política de grupo**. Se você não estiver interessado em monitorar os Dados de Recurso ou Dados de Processo, um ou ambos podem ser desativados usando a política de grupo. Para obter mais informações, consulte a seção **Política de Grupo** de Criar políticas.

**Preparação de dados**. As configurações padrão de retenção de dados podem ser modificadas para limpar os dados mais cedo e liberar espaço de armazenamento. Para obter mais informações sobre as configurações de preparação, consulte Granularidade e retenção de dados em Acessando dados usando a API.

## Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro

Nas versões VDA 7.0 a 7.8, as configurações de **Porta COM e Porta LPT** são configuráveis apenas usando o registro. Para versões VDA anteriores a 7.0 e para versões VDA 7.9 e posteriores, essas configurações são configuráveis no Web Studio. Para obter mais informações, consulte Configurações de política de redirecionamento de porta e Configurações de política de largura de banda.

As configurações de política para redirecionamento de porta COM e porta LPT estão localizadas em HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated na imagem ou máquina VDA.

Para habilitar o redirecionamento de porta COM e porta LPT, adicione novas chaves de registro do tipo REG_DWORD, da seguinte forma:

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

| CHAVE DO REGISTRO | DESCRIÇÃO | VALORES PERMITIDOS |
|---|---|---|
| AllowComPortRedirection | Permitir ou proibir o redirecionamento de porta COM | 1 (Permitir) ou 0 (Proibir) |
| LimitComBw | Limite de largura de banda para o canal de redirecionamento de porta COM | Valor numérico |

| CHAVE DO REGISTRO | DESCRIÇÃO | VALORES PERMITIDOS |
|---|---|---|
| LimitComBWPercent | Limite de largura de banda para o canal de redirecionamento de porta COM como uma porcentagem da largura de banda total da sessão | Valor numérico entre 0 e 100 |
| AutoConnectClientComPorts | Conectar automaticamente as portas COM do dispositivo do usuário | 1 (Permitir) ou 0 (Proibir) |
| AllowLptPortRedirection | Permitir ou proibir o redirecionamento da porta LPT | 1 (Permitir) ou 0 (Proibir) |
| LimitLptBw | Limite de largura de banda para o canal de redirecionamento da porta LPT | Valor numérico |
| LimitLptBwPercent | Limite de largura de banda para o canal de redirecionamento da porta LPT como uma porcentagem da largura de banda total da sessão | Valor numérico entre 0 e 100 |
| AutoConnectClientLptPorts | Conectar automaticamente as portas LPT do dispositivo do usuário | 1 (Permitir) ou 0 (Proibir) |

Após configurar essas configurações, altere seus catálogos de máquinas para usar a nova imagem mestre ou máquina física atualizada. Os desktops são atualizados com as novas configurações na próxima vez que os usuários fizerem logoff.

## Configurações de política do Connector para Configuration Manager 2012

A seção Connector para Configuration Manager 2012 contém configurações de política para configurar o agente Citrix Connector 7.5.

> **Importante:**
>
> As políticas de aviso, logoff e reinicialização aplicam-se apenas a implantações em catálogos de máquinas de SO de várias sessões que são gerenciados manualmente ou por Provisioning Services. Para esses catálogos de máquinas, o serviço Connector alerta os usuários quando há instalações de aplicativos pendentes ou atualizações de software.

> Para catálogos gerenciados por MCS, use o Web Studio para notificar os usuários. Para catálogos de SO de sessão única gerenciados manualmente, use o Configuration Manager para notificar os usuários. Para catálogos de SO de sessão única gerenciados por Provisioning Services, use o Provisioning Services para notificar os usuários.

### Intervalo de frequência de aviso

Essa configuração define o intervalo entre as aparições da mensagem de aviso para os usuários.

Os intervalos são definidos usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0–999.
- hh são horas com um intervalo de 0–23.
- mm são minutos com um intervalo de 0–59.
- ss são segundos com um intervalo de 0–59.

Por padrão, a configuração de intervalo é de 1 hora (01:00:00).

### Texto do corpo da caixa de mensagem de aviso

Essa configuração contém o texto editável da mensagem para os usuários, notificando-os sobre as próximas atualizações de software ou manutenção que exige que eles façam logoff.

Por padrão, a mensagem é: {TIMESTAMP} Salve seu trabalho. O servidor ficará offline para manutenção em {TIMELEFT}.

### Título da caixa de mensagem de aviso

Esta configuração contém o texto editável da barra de título da mensagem de aviso aos usuários.

Por padrão, o título é: Manutenção Futura

### Período de tempo do aviso

Esta configuração define quanto tempo antes da manutenção a mensagem de aviso aparece pela primeira vez.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração é de 16 horas (16:00:00), indicando que a primeira mensagem de aviso aparece aproximadamente 16 horas antes da manutenção.

### Texto do corpo da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da mensagem que alerta os usuários de que um logoff forçado foi iniciado.

Por padrão, a mensagem é: O servidor está atualmente ficando offline para manutenção

### Título da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da barra de título da mensagem final de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

### Período de carência para logoff forçado

Esta configuração define o período entre a notificação aos usuários para fazer logoff e a implementação do logoff forçado para processar a manutenção pendente.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração do período de carência para logoff forçado é de 5 minutos (00:05:00).

### Texto do corpo da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da mensagem que informa aos usuários para salvar seu trabalho e fazer logoff antes que um logoff forçado seja iniciado.

Por padrão, a mensagem contém o seguinte: {TIMESTAMP} Salve seu trabalho e faça logoff. O servidor ficará offline para manutenção em {TIMELEFT}.

### Título da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da barra de título da mensagem de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

### Modo gerenciado por imagem

O agente do Connector detecta automaticamente se está sendo executado em um clone de máquina gerenciado pelo Provisioning Services ou MCS. O agente bloqueia as atualizações do Configuration Manager em clones gerenciados por imagem e instala automaticamente as atualizações na imagem mestre do catálogo.

Depois que uma imagem mestre é atualizada, use o Web Studio para orquestrar a reinicialização dos clones do catálogo MCS. O Agente do Connector orquestra automaticamente a reinicialização dos clones do catálogo PVS durante as janelas de manutenção do Configuration Manager. Para substituir esse comportamento para que o software seja instalado em clones de catálogo pelo Configuration Manager, altere o Modo gerenciado por imagem para Desabilitado.

### Texto do corpo da caixa de mensagem de reinicialização

Essa configuração contém o texto editável da mensagem que notifica os usuários quando o servidor está prestes a ser reiniciado.

Por padrão, a mensagem é: O servidor está atualmente ficando offline para manutenção.

### Intervalo de tempo regular em que a tarefa do agente deve ser executada

Essa configuração determina a frequência com que a tarefa do agente Citrix Connector™ é executada.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.

- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração de intervalo de tempo regular é de 5 minutos (00:05:00).

## Alterações de política

A tabela a seguir lista as atualizações de política no Citrix Virtual Apps and Desktops™ 7 2402, incluindo adições, remoções, alterações de nome e alterações de estado padrão.

| CONFIGURAÇÃO DE POLÍTICA | ALTERAÇÕES |
| --- | --- |
| Configurações de política de impressoras cliente > Impressoras cliente retidas e restauradas | Obsoleto em 2402 |

**Observação:**

Exclua todas as configurações obsoletas antes de atualizar. Se alguma configuração obsoleta permanecer em uso, a atualização poderá falhar com um erro.

# Gerenciar

O gerenciamento de um site Citrix Virtual Apps and Desktops™ abrange vários itens e tarefas.

### Licenciamento

É necessária uma conexão válida com o Servidor de Licenças Citrix ao criar um site. Posteriormente, você pode concluir várias tarefas de licenciamento no Studio, incluindo adicionar licenças, alterar tipos ou modelos de licença e gerenciar administradores de licença. Você também pode acessar o Console de Administração de Licenças no Studio.

### Aplicativos

Gerencie aplicativos em Delivery Groups e, opcionalmente, em Application Groups.

### Zonas

Em uma implantação geograficamente dispersa, você pode usar zonas para manter aplicativos e desktops mais próximos dos usuários finais, o que pode melhorar o desempenho. Ao instalar e configurar um site, todos os Controladores, catálogos de máquinas e conexões de host estão em uma zona primária. Posteriormente, você pode usar o Studio para criar zonas satélite contendo esses itens. Depois que seu site tiver mais de uma zona, você poderá indicar em qual zona quaisquer catálogos de máquinas recém-criados, conexões de host ou Controladores adicionados serão colocados. Você também pode mover itens entre zonas.

### Conexões e recursos

Se você estiver usando um hipervisor ou outro serviço para hospedar máquinas que fornecem aplicativos e desktops aos usuários, você cria sua primeira conexão com esse hipervisor ou outro serviço ao criar um site. Os detalhes de armazenamento e rede para essa conexão formam seus recursos. Posteriormente, você pode alterar essa conexão e seus recursos, e criar mais conexões. Você também pode gerenciar as máquinas que usam uma conexão configurada.

### Cache de Host Local

O Cache de Host Local permite que as operações de intermediação de conexão em um site continuem quando a conexão entre um Delivery Controller™ e o banco de dados do site falha.

### IP virtual e loopback virtual

O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem de comunicações com localhost para usar um endereço de loopback virtual exclusivo no intervalo de localhost.

### Controladores de Entrega

Este artigo contém considerações e procedimentos ao adicionar e remover Controladores de um site. Ele também descreve como mover Controladores para outra zona ou site, e como mover um VDA para outro site.

### Registro de VDA com Controladores

Antes que um VDA possa ajudar a entregar aplicativos e desktops, ele deve se registrar (estabelecer comunicação) com um Controlador. Os endereços do Controlador podem ser especificados de várias maneiras, que são descritas neste artigo. É fundamental que os VDAs tenham informações atualizadas à medida que os Controladores são adicionados, movidos e removidos no site.

### Sessões

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência do usuário. Vários recursos podem otimizar a confiabilidade das sessões, reduzir inconvenientes, tempo de inatividade e perda de produtividade.

- Confiabilidade da sessão
- Reconexão automática do cliente
- ICA® Keep-Alive
- Controle de workspace
- Roaming de sessão

### Usar pesquisa no Studio

Quando você quiser visualizar informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou Delivery Groups no Studio, use o recurso de pesquisa flexível.

### Tags

Use tags para identificar itens como máquinas, aplicativos, grupos e políticas. Você pode então adaptar certas operações para aplicar apenas a itens com uma tag específica.

### IPv4/IPv6

O Citrix Virtual Apps and Desktops oferece suporte a implantações IPv4 puro, IPv6 puro e dual-stack que usam redes IPv4 e IPv6 sobrepostas. Este artigo descreve e ilustra essas implantações. Ele também descreve as configurações de política do Citrix que controlam o uso de IPv4 ou IPv6.

### Perfis de usuário

Por padrão, o Citrix Profile Management é instalado automaticamente quando você instala um VDA. Se você usa essa solução de perfil, revise este artigo para obter informações gerais. Consulte a documentação do Profile Management para obter detalhes.

#### Coletar rastreamentos do Citrix Diagnostic Facility (CDF)

O utilitário CDFControl é um controlador ou consumidor de rastreamento de eventos para capturar mensagens de rastreamento do Citrix Diagnostic Facility (CDF) exibidas por vários provedores de rastreamento Citrix. Ele foi feito para solucionar problemas complexos relacionados ao Citrix, oferecer suporte a filtros de análise e coletar dados de desempenho.

### Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios.

#### Citrix Scout

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manutenção proativa em sua implantação do Citrix Virtual Apps and Desktops. O Citrix oferece análise abrangente e automatizada de coleções de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

# Aplicativos

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

## Introdução

Se sua implantação usa apenas grupos de entrega (e não grupos de aplicativos), você adiciona aplicativos aos grupos de entrega. Se você também tiver grupos de aplicativos, geralmente adiciona aplicativos aos grupos de aplicativos. Essa orientação facilita a administração. Um aplicativo deve sempre pertencer a pelo menos um grupo de entrega ou grupo de aplicativos.

No assistente Adicionar Aplicativos, você pode selecionar um ou mais grupos de entrega, ou um ou mais grupos de aplicativos, mas não ambos. Embora você possa alterar posteriormente a associação de grupo de um aplicativo (por exemplo, mover um aplicativo de um grupo de aplicativos para um grupo de entrega), a melhor prática desencoraja adicionar essa complexidade. Mantenha seus aplicativos em um único tipo de grupo.

Quando você associa um aplicativo a mais de um grupo, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo está associado.

Se você publicar dois aplicativos com o mesmo nome (talvez de grupos diferentes) para os mesmos usuários, altere a propriedade `Application name (for user)` no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace™.

Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Você também pode alterar a pasta do aplicativo onde o aplicativo é colocado, seja ao adicionar o aplicativo ou posteriormente.

Para obter detalhes, consulte:

- Criar grupos de entrega
- Criar grupos de aplicativos
- Tags

## Adicionar aplicativos

Você pode adicionar aplicativos ao criar um grupo de entrega ou um grupo de aplicativos. Esses procedimentos são detalhados em Criar grupos de entrega e Criar grupos de aplicativos. O procedimento a seguir descreve como adicionar aplicativos depois de criar um grupo.

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega de Acesso Remoto a PC.

- Você não pode usar o assistente Adicionar Aplicativo para remover aplicativos de grupos de entrega ou grupos de aplicativos. Essa é uma operação separada.

Para adicionar um ou mais aplicativos:

1. Selecione **Aplicativos** no painel esquerdo e então selecione **Adicionar Aplicativos** na barra de ações.
2. O assistente Adicionar Aplicativos é iniciado com uma página de **Introdução**, que você pode remover de futuras inicializações deste assistente.
3. O assistente o guiará pelas páginas **Grupos**, **Aplicativos** e **Resumo**. Quando terminar cada página, clique em **Avançar** até chegar à página **Resumo**.

Alternativas à etapa 1 se você quiser adicionar aplicativos a um único grupo de entrega ou grupo de aplicativos:

- **Para adicionar aplicativos a apenas um grupo de entrega:** Na etapa 1, selecione **Grupos de Entrega** no painel esquerdo do Web Studio, selecione um grupo de entrega no painel central e então selecione **Adicionar Aplicativos** na barra de ações. O assistente não exibe a página **Grupos**.
- **Para adicionar aplicativos a apenas um grupo de aplicativos:** Na etapa 1, selecione **Aplicativos** no painel esquerdo do Web Studio, selecione um grupo de aplicativos no painel central e então selecione a entrada **Adicionar Aplicativos** abaixo do nome do grupo de aplicativos na barra de ações. O assistente não exibe a página **Grupos**.

### Página Grupos

Esta página lista todos os grupos de entrega no site. Se você também criou grupos de aplicativos, a página lista os grupos de aplicativos e os grupos de entrega. Você pode escolher entre um dos grupos, mas não de ambos os grupos. Em outras palavras, você não pode adicionar aplicativos a um grupo de aplicativos e a um grupo de entrega ao mesmo tempo. Geralmente, se você estiver usando grupos de aplicativos, adicione aplicativos a grupos de aplicativos, em vez de grupos de entrega.

Ao adicionar um aplicativo, selecione a caixa de seleção ao lado de pelo menos um grupo de entrega (ou grupo de aplicativos, se disponível). Todo aplicativo deve estar sempre associado a pelo menos um grupo.

### Página Aplicativos

Clique em **Adicionar** para exibir as fontes do aplicativo.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Quando você seleciona esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Selecione as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se você (1) selecionou grupos de aplicativos sem grupos de entrega associados, (2) selecionou grupos de aplicativos com grupos de entrega associados que não contêm máquinas, ou (3) selecionou um grupo de entrega que não contém máquinas.

- **Manualmente:** Aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. A seleção desta origem abre uma nova página onde você especifica um aplicativo a ser adicionado das seguintes maneiras:

  - Digite o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Procurar**, insira as credenciais para acessar o VDA, aguarde a conexão com o VDA e então selecione um aplicativo do VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.

- **Existente:** Aplicativos adicionados anteriormente ao site. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se o site não tiver aplicativos.

- **Pacotes de aplicativos:** Aplicativos em pacotes de aplicativos App-V, MSIX, MSIX app attach ou FlexApp. Ao selecionar esta origem, a página **Adicionar Aplicativos de Pacotes** é aberta. Selecione uma origem de pacote de aplicativos, selecione os aplicativos que deseja adicionar na exibição resultante e, em seguida, selecione **OK**. Para obter mais informações, consulte Implantar e entregar pacotes de aplicativos.

- **Grupo de Aplicativos**: Grupos de aplicativos. Ao selecionar esta origem, uma nova página é aberta com uma lista de grupos de aplicativos. (Embora a exibição também liste os aplicativos em cada grupo, você pode selecionar apenas o grupo, não aplicativos individuais.) Todos os aplicativos atuais e futuros nos grupos selecionados são adicionados. Marque as caixas de seleção dos grupos de aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se (1) não houver grupos de aplicativos ou (2) se os grupos de entrega selecionados não suportarem grupos de aplicativos (por exemplo, grupos de entrega com máquinas atribuídas estaticamente).

Conforme observado na tabela, algumas origens na lista **Adicionar** não podem ser selecionadas se não houver uma origem válida desse tipo. Origens incompatíveis (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos) não são incluídas na lista. Os aplicativos que já foram adicionados aos grupos que você escolheu não podem ser selecionados.

Você pode alterar as propriedades (configurações) de um aplicativo a partir desta página ou posteriormente.

Por padrão, os aplicativos adicionados são colocados na pasta de aplicativos chamada `Applications`. Você pode alterar o aplicativo a partir desta página ou posteriormente. Se você tentar adicionar um aplicativo e um com o mesmo nome já existir na mesma pasta, será solicitado que você renomeie o aplicativo que está adicionando. Você pode aceitar o novo nome oferecido, ou recusar e então renomear o aplicativo ou selecionar uma pasta diferente. Por exemplo, se `app` já existe na pasta **Aplicativos**, e você tentar adicionar outro aplicativo chamado `app` a essa pasta, o novo nome `app_1` será oferecido.

### Página de resumo

Se você estiver adicionando 10 ou menos aplicativos, seus nomes serão listados em **Aplicativos a adicionar**. Se você estiver adicionando mais de 10 aplicativos, o número total será especificado.

Revise as informações de resumo e clique em **Concluir**.

## Alterar a associação de grupo de um aplicativo

Após adicionar um aplicativo, você pode alterar os grupos de entrega e os grupos de aplicativos aos quais o aplicativo está associado.

Você pode arrastar um aplicativo para um grupo adicional. Esta é uma alternativa ao uso de comandos na barra de ações.

Se um aplicativo estiver associado a mais de um grupo de entrega ou grupo de aplicativos, a prioridade do grupo pode ser usada para especificar a ordem em que vários grupos são verificados para encontrar aplicativos. Por padrão, todos os grupos têm prioridade 0 (a mais alta). Grupos com a mesma prioridade são balanceados por carga.

Um aplicativo pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos. Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se (1) o grupo de entrega contiver máquinas compartilhadas e tiver sido criado com uma versão do XenDesktop 7.x anterior à 7.9, e (2) você tiver a permissão `Edit delivery group`. O tipo de grupo de entrega é

automaticamente convertido para `desktops and applications` quando a caixa de diálogo de propriedades é confirmada.

1. Faça login no Web Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione o aplicativo.
2. Selecione **Propriedades** na barra de ações.
3. Selecione a página **Grupos**.
    - Para adicionar um grupo, clique em **Adicionar** e selecione **Grupos de Aplicativos** ou **Grupos de Entrega**. (Se você não criou nenhum grupo de aplicativos, a única entrada é **Grupos de Entrega**.) Em seguida, selecione um ou mais grupos disponíveis. Grupos que são incompatíveis com o aplicativo, ou que já estão associados ao aplicativo, não podem ser selecionados.
    - Para remover um grupo, selecione um ou mais grupos e clique em **Remover**. Se a remoção da associação do grupo resultar na não associação do aplicativo a nenhum grupo, você será alertado de que o aplicativo será excluído.
    - Para alterar a prioridade de um grupo, selecione o grupo e clique em **Editar Prioridade**. Selecione um valor de prioridade e clique em **OK**.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações e deixar a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

## Duplicar, habilitar ou desabilitar, renomear ou excluir um aplicativo

As seguintes ações estão disponíveis:

- **Duplicar:** Você pode querer duplicar um aplicativo para criar uma versão diferente com parâmetros ou propriedades diferentes. Ao duplicar um aplicativo, ele é automaticamente renomeado com um sufixo exclusivo e colocado ao lado do original. Você também pode querer duplicar um aplicativo e depois adicioná-lo a um grupo diferente. (Após a duplicação, a maneira mais fácil de mover um aplicativo é arrastando-o.)
- **Habilitar ou desabilitar:** Habilitar e desabilitar um aplicativo é uma ação diferente de habilitar e desabilitar um grupo de entrega ou grupo de aplicativos.
- **Renomear:** Você pode renomear apenas um aplicativo por vez. Se você tentar renomear um aplicativo e um com o mesmo nome existir na mesma pasta ou grupo, será solicitado que você especifique um nome diferente.
- **Excluir:** A exclusão de um aplicativo o remove dos grupos de entrega e grupos de aplicativos aos quais ele estava associado, mas não da origem que foi usada para adicionar o aplicativo

originalmente. Excluir um aplicativo é uma ação diferente de removê-lo de um grupo de entrega ou grupo de aplicativos.

Para duplicar, habilitar, desabilitar, renomear ou excluir um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um ou mais aplicativos no painel central e, em seguida, selecione a tarefa apropriada na barra de ações.
3. Confirme a ação, quando solicitado.

## Remover aplicativos de um grupo de entrega

Um aplicativo deve estar associado (pertencer) a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de entrega que removeria a associação desse aplicativo com qualquer grupo de entrega ou grupo de aplicativos, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente de uma fonte válida.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo de entrega. No painel central inferior, na guia **Aplicativos**, selecione o aplicativo que deseja remover.
3. Selecione **Remover Aplicativo** na barra de ações.
4. Confirme a remoção.

## Remover aplicativos de um grupo de aplicativos

Um aplicativo deve pertencer a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de aplicativos que resultará na não pertença desse aplicativo a nenhum grupo, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente de uma fonte válida.

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione o grupo de aplicativos no painel central e, em seguida, selecione um ou mais aplicativos.
3. Selecione **Remover do Grupo de Aplicativos** na barra de ações.
4. Confirme a remoção.

# Alterar propriedades do aplicativo

Você pode alterar as propriedades de apenas um aplicativo por vez.

Para alterar as propriedades de um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** na barra de ações.
3. Selecione a página que contém a propriedade que você deseja alterar.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Na lista a seguir, a página é mostrada entre parênteses.

| PROPRIEDADE | PÁGINA |
|---|---|
| Categoria/pasta onde o aplicativo aparece no aplicativo Citrix Workspace | Entrega |
| Argumentos de linha de comando; consulte Passar parâmetros para aplicativos publicados | Localização |
| Grupos de entrega e grupos de aplicativos onde o aplicativo está disponível | Grupos |
| Descrição | Identificação |
| Extensões de nome de arquivo e associação de tipo de arquivo: quais extensões o aplicativo abre automaticamente | Associação de Tipo de Arquivo |
| Ícone | Entrega |
| Palavras-chave para StoreFront™ | Identificação |
| Limites; consulte Configurar limites de aplicativo | Entrega |
| Nome: Nomes vistos pelo usuário e pelo administrador | Identificação |

| PROPRIEDADE | PÁGINA |
| --- | --- |
| Caminho para o executável; consulte Passar parâmetros para aplicativos publicados | Localização |
| Atalho na área de trabalho do usuário: habilitar ou desabilitar | Entrega |
| Visibilidade: Limita quais usuários podem ver o aplicativo no aplicativo Citrix Workspace. Um aplicativo invisível ainda pode ser iniciado. Para torná-lo indisponível e invisível, adicione-o a um grupo diferente. | Limitar Visibilidade |
| Diretório de trabalho | Localização |

As alterações do aplicativo podem não ter efeito para os usuários atuais do aplicativo até que eles saiam de suas sessões.

## Configurar limites de aplicativo

Configure limites de aplicativo para ajudar a gerenciar o uso do aplicativo. Por exemplo, você pode usar limites de aplicativo para gerenciar o número de usuários acessando um aplicativo simultaneamente. Da mesma forma, os limites de aplicativo podem ser usados para gerenciar o número de instâncias simultâneas de aplicativos que consomem muitos recursos. Esse limite pode ajudar a manter o desempenho do servidor e evitar a deterioração do serviço.

Este recurso limita o número de inicializações de aplicativos que são intermediadas pelo Controller (por exemplo, do aplicativo Citrix Workspace e do StoreFront), e não o número de aplicativos em execução que podem ser iniciados por outros métodos. Isso significa que os limites de aplicativo auxiliam os administradores no gerenciamento do uso simultâneo, mas não fornecem aplicação em todos os cenários. Por exemplo, os limites de aplicativo não podem ser aplicados quando o Controller está no modo de interrupção.

Por padrão, não há limite para quantas instâncias de aplicativo podem ser executadas ao mesmo tempo. Existem várias configurações de limite de aplicativo. Você pode configurar qualquer uma ou todas elas.

- O número máximo de instâncias simultâneas do aplicativo por todos os usuários no grupo de entrega.
- Uma instância do aplicativo por usuário no grupo de entrega.

- O número máximo de instâncias simultâneas do aplicativo por máquina (somente PowerShell).

Se um limite for configurado, uma mensagem de erro será gerada quando um usuário tentar iniciar uma instância do aplicativo que excederá o limite configurado. Se mais de um limite for configurado, um erro será relatado quando o primeiro limite for atingido.

Exemplos de uso de limites de aplicativo:

- **Limite máximo de instâncias simultâneas:** Em um grupo de entrega, você configura o número máximo de instâncias simultâneas do aplicativo `Alpha` para 15. Mais tarde, os usuários nesse grupo de entrega têm 15 instâncias desse aplicativo em execução ao mesmo tempo. Se qualquer usuário nesse grupo de entrega agora tentar iniciar `Alpha`, uma mensagem de erro será gerada. `Alpha` não é iniciado porque excederia o limite configurado de instâncias simultâneas de aplicativo (15).
- **Limite de aplicativo de uma instância por usuário:** Em outro grupo de entrega, você habilita a opção de uma instância por usuário para o aplicativo `Beta`. O usuário Tony inicia o aplicativo `Beta` com sucesso. Mais tarde no dia, enquanto esse aplicativo ainda está em execução na sessão de Tony, ele tenta iniciar outra instância de `Beta`. Uma mensagem de erro é gerada e `Beta` não é iniciado porque excederia o limite de uma instância por usuário.
- **Número máximo de instâncias simultâneas e limites de uma instância por usuário:** Em outro grupo de entrega, você configura um número máximo de instâncias simultâneas de 10 e habilita a opção de uma instância por usuário para o aplicativo `Delta`. Mais tarde, quando 10 usuários nesse grupo de entrega tiverem uma instância de `Delta` em execução, qualquer outro usuário nesse grupo de entrega que tentar iniciar `Delta` receberá uma mensagem de erro. `Delta` não é iniciado. Se qualquer um dos 10 usuários atuais de `Delta` tentar iniciar uma segunda instância desse aplicativo, eles receberão uma mensagem de erro e a segunda instância não será iniciada.
- **Número máximo de instâncias simultâneas por máquina e uso de restrições de tag:** O aplicativo `Charlie` tem requisitos de licenciamento e desempenho que ditam quantas instâncias podem estar em execução ao mesmo tempo em um servidor específico. Esses requisitos também ditam quantas instâncias podem estar em execução simultaneamente em todos os servidores do site.

  O limite de instâncias de aplicativo por máquina afeta qualquer servidor no site (não apenas máquinas em um grupo de entrega específico). Digamos que seu site tenha três servidores. Para o aplicativo `Charlie`, você configura o limite de instâncias de aplicativo por máquina para 2. Assim, não mais do que seis instâncias do aplicativo `Charlie` podem ser iniciadas

em todo o site. (Isso é um limite de duas instâncias de Charlie em cada um dos três servidores.)

Para restringir o uso de um aplicativo a apenas certas máquinas dentro de um grupo de entrega (além de limitar as instâncias em todas as máquinas em todo o site):

- Use a funcionalidade de marcação para essas máquinas.
- Configure o número máximo de instâncias por limite de máquina para essa aplicação.

Se as aplicações forem iniciadas por métodos diferentes da intermediação do Controlador (por exemplo, enquanto um Controlador estiver em modo de interrupção) e os limites configurados forem excedidos, os usuários não poderão iniciar mais instâncias até que fechem instâncias suficientes para não exceder mais os limites. As instâncias que excederam o limite não são encerradas à força. Elas terão permissão para continuar até que seus usuários as fechem.

Se você desabilitar o roaming de sessão, desabilite o limite de uma instância por usuário para a aplicação. Se você habilitar o limite de uma instância por usuário para a aplicação, não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos. Para obter informações sobre roaming, consulte Sessões.

Para configurar o limite máximo de instâncias por grupo de entrega e o limite de uma instância por usuário:

1. Selecione **Aplicações** no painel esquerdo e, em seguida, selecione uma aplicação.
2. Selecione **Editar Propriedades da Aplicação** na barra de ações.
3. Na página **Entrega**, escolha uma das seguintes opções.

   - **Permitir uso ilimitado da aplicação**. Não há limite para o número de instâncias em execução ao mesmo tempo. Este é o padrão.
   - **Definir limites para a aplicação**. Existem dois tipos de limite; especifique um ou ambos.
     - Especifique o número máximo de instâncias que podem ser executadas simultaneamente por máquina
     - Limitar a uma instância da aplicação por usuário

4. Clique em **OK** para aplicar a alteração e fechar a caixa de diálogo, ou em **Aplicar** para aplicar a alteração e deixar a caixa de diálogo aberta.

Para configurar o limite máximo de instâncias por máquina (somente PowerShell):

- No PowerShell (usando o Remote PowerShell SDK para implantações do Citrix Cloud™ ou o PowerShell SDK para implantações locais), insira o `BrokerApplication` cmdlet apropriado com o parâmetro `MaxPerMachineInstances`.
- Para orientação, use o cmdlet `Get-Help`. Por exemplo:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

## Passar parâmetros para aplicativos publicados

Use a página **Local** das propriedades de um aplicativo para inserir a linha de comando e passar parâmetros para aplicativos publicados.

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos `"%*"` (símbolos de porcentagem e asterisco entre aspas duplas) são anexados ao final da linha de comando do aplicativo. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos de usuário.

Se um aplicativo publicado não iniciar conforme o esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos de usuário são validados quando os símbolos `"%*"` são anexados. Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo de usuário, os símbolos `"%**"` são anexados à linha de comando para ignorar a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como `"C:\Program Files"`), coloque a linha de comando do aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Para fazer isso, adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos `%*`. Certifique-se de incluir um espaço entre a aspa de fechamento do caminho e a aspa de abertura para os símbolos `%*`.

Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **Nota:**
>
> O número máximo de caracteres, incluindo argumentos, na linha de comando para iniciar aplicativos publicados é 203.

## Gerenciar pastas de aplicativos

Por padrão, os novos aplicativos que você adiciona a grupos de entrega são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente ao criar o grupo de entrega, ao adicionar um aplicativo ou posteriormente.

É bom saber:

- Você não pode renomear ou excluir a pasta Aplicativos, mas pode mover todos os aplicativos que ela contém para outras pastas que você criar.
- Um nome de pasta pode conter 1 a 64 caracteres. Espaços são permitidos.
- As pastas podem ser aninhadas em até cinco níveis.
- As pastas não precisam conter aplicativos. Pastas vazias são permitidas.
- As pastas são listadas em ordem alfabética no Web Studio, a menos que você as mova ou especifique um local diferente ao criá-las.
- Você pode ter mais de uma pasta com o mesmo nome, desde que cada uma tenha uma pasta pai diferente. Da mesma forma, você pode ter mais de um aplicativo com o mesmo nome, desde que cada um esteja em uma pasta diferente.
- Você deve ter a permissão `View Applications` para ver os aplicativos nas pastas, e deve ter a permissão `Edit Application Properties` para todos os aplicativos na pasta para remover, renomear ou excluir uma pasta que contém aplicativos.
- A maioria dos procedimentos a seguir solicita ações usando a barra de ações no Web Studio. Alternativamente, você pode usar menus de clique com o botão direito ou arrastar o item. Por exemplo, se você criar ou mover uma pasta para um local não intencional, você pode arrastá-la/soltá-la para o local correto.
- Todos os nós no Web Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Aplicativos**, você deve adicionar os metadados `ContainsApplications` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplications -Value true
```

Para gerenciar pastas de aplicativos, selecione **Aplicativos** no painel esquerdo. Use a lista a seguir como guia.

- **Para visualizar todas as pastas (excluindo pastas aninhadas):** Clique em **Mostrar tudo** acima da lista de pastas.
- **Para criar uma pasta no nível mais alto (não aninhada):** Selecione a pasta **Aplicativos**. Para colocar a nova pasta sob uma pasta existente diferente de **Aplicativos**, selecione essa pasta. Em seguida, selecione **Criar Pasta** na barra de ações. Digite um nome.
- **Para mover uma pasta:** Selecione a pasta e, em seguida, selecione **Mover Pasta** na barra de ações. Você pode mover apenas uma pasta por vez, a menos que a pasta contenha pastas aninhadas. (A maneira mais fácil de mover uma pasta é arrastá-la.)
- **Para renomear uma pasta:** Selecione a pasta e, em seguida, selecione **Renomear Pasta** na barra de ações. Digite um nome.
- **Para excluir uma pasta:** Selecione a pasta e, em seguida, selecione **Excluir Pasta** na barra de ações. Ao excluir uma pasta que contém aplicativos e outras pastas, esses objetos também são excluídos. A exclusão de um aplicativo remove a atribuição do aplicativo do grupo de entrega. Isso não o remove da máquina.
- **Para mover aplicativos para uma pasta:** Selecione um ou mais aplicativos. Em seguida, selecione **Mover Aplicativo** na barra de ações. Selecione a pasta.

Você também pode colocar os aplicativos que está adicionando em uma pasta na página **Aplicativo** ao criar um grupo de entrega ou um grupo de aplicativos. Por padrão, os aplicativos adicionados vão para a pasta **Aplicativos**. Clique em **Alterar** para selecionar ou criar uma pasta.

## Controlar o lançamento local de aplicativos em desktops publicados

Quando os usuários iniciam um aplicativo publicado de dentro de um desktop publicado, você pode controlar se o aplicativo é iniciado nessa sessão de desktop ou como um aplicativo publicado. O aplicativo Citrix Workspace procura o caminho de instalação do aplicativo no registro do Windows no VDA e, se presente, inicia a instância local do aplicativo. Caso contrário, uma instância hospedada do aplicativo é iniciada. Se você iniciar um aplicativo que não está instalado no VDA, o aplicativo hospedado será iniciado. Para obter mais informações, consulte início vPrefer.

No PowerShell (usando o SDK do PowerShell Remoto em implantações do Citrix Cloud ou o SDK do PowerShell em implantações locais), você pode alterar esta ação.

No cmdlet `New-Broker` Application ou `Set-BrokerApplication`, use a opção `LocalLaunchDisabled`. Por exemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Por padrão, o valor desta opção é false (`-LocalLaunchDisabled $false`). Ao iniciar um aplicativo publicado de dentro de um desktop publicado, o aplicativo é iniciado nessa sessão de desktop.

Se você definir o valor da opção como true (`-LocalLaunchDisabled $true`), o aplicativo publicado será iniciado. Isso cria uma sessão separada e adicional do desktop publicado (usando o aplicativo Citrix Workspace para Windows) para o aplicativo publicado.

Requisitos e limites:

- O valor `ApplicationType` do aplicativo deve ser `HostedOnDesktop`.
- Esta opção está disponível apenas através do SDK do PowerShell apropriado. Atualmente, não está disponível na interface gráfica do Web Studio.
- Esta opção requer no mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 e Delivery Controller 7.17.

## Pacotes de aplicativos

> **Nota:**

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

> A Microsoft fornece três tecnologias de empacotamento para entregar aplicativos aos usuários: App-V, MSIX e MSIX app attach. Este artigo orienta você sobre como implantar e entregar esses aplicativos empacotados usando **Web Studio > App Packages**:

- Implantar e entregar aplicativos App-V

- Implantar e entregar aplicativos MSIX e MSIX app attach

## Implantar e entregar aplicativos App-V

Esta seção aborda as seguintes informações:

- Visão geral. Descreve os métodos de gerenciamento para entregar e gerenciar os pacotes App-V.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

### Visão geral

Esta seção descreve os métodos de gerenciamento para entregar e gerenciar os pacotes App-V. Para obter mais informações sobre os componentes e conceitos com os quais você interage ao entregar aplicativos empacotados App-V, consulte a documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/application-management/app-v/appv-for-windows>`.

Você pode usar os seguintes métodos para entregar e gerenciar pacotes App-V:

- **Dual Admin**. Os pacotes de aplicativos são configurados e gerenciados em servidores App-V. O Citrix Virtual Apps and Desktops e os servidores App-V trabalham juntos para entregar e gerenciar pacotes.

  Este método exige que o Citrix Virtual Apps and Desktops atualize periodicamente a visualização do instantâneo do estado do servidor App-V. Ele incorre em sobrecarga de hardware, infraestrutura e administração. O Citrix Virtual Apps and Desktops e os servidores App-V devem permanecer sincronizados, particularmente para permissões de usuário.

  O Dual Admin funciona melhor em implantações onde o App-V e seu ambiente estão intimamente acoplados:

  - **Servidor de gerenciamento App-V**. Publica e gerencia o ciclo de vida dos pacotes App-V e dos Arquivos de Configuração Dinâmica.
  - **Componente de Personalização Citrix** instalado em máquinas VDA. Gerencia o registro do servidor de publicação App-V apropriado necessário para o lançamento de aplicativos.

  Este método garante que o servidor de publicação App-V seja sincronizado para o usuário no momento apropriado. O servidor de publicação mantém outros aspectos do ciclo de vida do pacote, como atualização no logon e grupos de conexão.
- **Administrador Único**. Os pacotes de aplicativos são armazenados em compartilhamentos de rede. O Citrix Virtual Apps and Desktops entrega e gerencia pacotes de forma independente.

Este método reduz a sobrecarga porque os servidores App-V e a infraestrutura de banco de dados não são necessários na implantação.

Neste método, você armazena pacotes App-V em um compartilhamento de rede e carrega seus metadados desse local para o seu ambiente. O componente Citrix Personalization instalado nas máquinas VDA então gerencia e entrega aplicativos da seguinte forma:

- Processar os Arquivos de Configuração de Implantação e os Arquivos de Configuração do Usuário quando um aplicativo é iniciado.
- Gerenciar todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Você pode usar ambos os métodos de gerenciamento simultaneamente. Em outras palavras, ao adicionar aplicativos a grupos de entrega, os aplicativos podem vir de pacotes App-V presentes em servidores App-V ou em compartilhamentos de rede.

> **Nota:**
>
> Se você estiver usando ambos os métodos de gerenciamento simultaneamente e o pacote App-V tiver um Arquivo de Configuração Dinâmica em ambos os locais, o arquivo no servidor App-V (Administrador Duplo) será usado.

**Procedimentos**

Para oferecer suporte à entrega de aplicativos App-V, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization em máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados App-V aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.
4. Para habilitar a entrega automática de pacotes App-V interdependentes, crie grupos de isolamento.

Para que o Citrix Virtual Apps and Desktops reconheça e aplique Arquivos de Configuração Dinâmica do App-V no método de Administrador Único, consulte este blog da Citrix.

## Implantar e entregar aplicativos MSIX e MSIX app attach

Esta seção abrange as seguintes informações:

- Visão geral. Descreve como os pacotes MSIX e MSIX app attach são entregues e gerenciados.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

### Visão geral

O Citrix Virtual Apps and Desktops entrega aplicativos MSIX e MSIX app attach aos usuários por meio do componente Citrix Personalization instalado nas máquinas VDA. Este componente gerencia todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Para obter mais informações sobre MSIX e MSIX app attach, consulte a documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/msix/>` e `<https://docs.microsoft.com/pt-br/azure/virtual-desktop/what-is-app-attach>` respectivamente.

### Procedimentos

Para oferecer suporte à entrega de pacotes MSIX e MSIX app attach, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization nas máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados MSIX e MSIX app attach aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.

## Instalar o componente Citrix Personalization nas máquinas VDA

O componente Citrix Personalization gerencia o processo de publicação de pacotes de aplicativos nos formatos App-V, MSIX e MSIX app attach. Este componente não é instalado por padrão ao instalar um VDA. Você pode instalar o componente durante ou após a instalação do VDA.

Para instalar o componente durante a instalação do VDA, use uma das seguintes maneiras:

- No assistente de instalação, vá para a página **Componentes Adicionais** e selecione a caixa de seleção **Citrix Personalization for App-V - VDA**.

- Na interface de linha de comando, use a opção **/includeadditional "Citrix Personalization for App-V – VDA"**.

Para instalar o componente após a instalação do VDA, siga estas etapas:

1. Na máquina VDA, vá para **Painel de Controle > Programas > Programas e Recursos**, clique com o botão direito em **Citrix Virtual Delivery Agent** e selecione **Alterar**.
2. No assistente que aparece, prossiga para a página **Componentes Adicionais** e, em seguida, ative a caixa de seleção **Citrix Personalization for App-V - VDA**.

> **Nota:**
>
> O Microsoft App-V Desktop Client é o componente que executa aplicativos virtuais de pacotes App-V em dispositivos de usuário. O Windows 10 (1607 ou posterior), o Windows Server 2016 e o Windows Server 2019 já incluem este software cliente App-V. Você só precisa habilitá-lo nas máquinas VDA. Para obter mais informações, consulte este artigo da documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>`.

### Armazenar pacotes de aplicativos em compartilhamentos de rede

Depois de configurar a infraestrutura, gere os pacotes de aplicativos e armazene-os em um local de rede, como um compartilhamento de rede UNC ou SMB, ou em um Azure File Share.

As etapas detalhadas são as seguintes:

1. Gere pacotes de aplicativos. Consulte a documentação da Microsoft para obter detalhes.
2. Armazene pacotes de aplicativos em um local de rede:
   - Para **App-V Single Admin**: Armazene os pacotes e os arquivos de configuração dinâmica correspondentes (App-V) em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
   - Para **App-V Dual Admin**: Publique os pacotes no servidor de gerenciamento App-V a partir de um caminho UNC. (A publicação a partir de URLs HTTP não é suportada.)
   - Para **MSIX ou MSIX app attach**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Azure File Share.
3. Certifique-se de que o VDA tenha permissão de leitura no caminho de armazenamento do pacote:

- Se você armazenar pacotes em um compartilhamento de rede UNC ou SMB em seu domínio AD, conceda à máquina VDA permissão de leitura para o caminho de armazenamento. Para fazer isso, você pode dar à conta AD da máquina permissão de leitura para o compartilhamento explicitamente, ou incluir a conta em um grupo AD que tenha essa permissão.
- Se você armazenar pacotes em um Azure File Share, primeiro conceda a uma conta de usuário permissão de leitura para o caminho de armazenamento no Azure. Em seguida, configure `ctxAppVService` em execução na máquina VDA para usar essa conta de usuário para acessar o caminho de armazenamento do pacote. Consulte a seção a seguir para obter as etapas detalhadas.

#### Alterar a conta de logon do usuário

O VDA chama `ctxAppVService` para acessar os caminhos de armazenamento de pacotes. Por padrão, `ctxAppVService` acessa os caminhos de armazenamento de pacotes usando a **conta do Sistema Local** da máquina. Esse tipo de autenticação de máquina funciona em domínios AD. No entanto, não funciona nos cenários de integração AD e Azure AD, que exigem autenticação baseada em conta de usuário.

Se você armazenar pacotes em um Azure File Share, altere a conta de logon para `ctxAppVService` para uma conta de usuário que tenha permissão de leitura no caminho de armazenamento do pacote. As etapas detalhadas são as seguintes:

1. Inicie **Serviços**, clique com o botão direito em **ctxAppVService** e selecione **Propriedades**.
2. Na guia **Fazer logon**, selecione **Esta conta**, insira uma conta de usuário que tenha permissão de leitura para o caminho de armazenamento do pacote e, em seguida, insira a senha do usuário duas vezes.
3. Clique em **OK**.

### Carregar pacotes de aplicativos para o seu ambiente

Depois de armazenar os pacotes de aplicativos em um local de rede conforme necessário, carregue-os para o seu ambiente para entrega. Use um dos seguintes métodos conforme necessário:

- Carregar em massa
- Carregar um por um

### Preparações

O Citrix Virtual Apps and Desktops usa uma máquina VDA para configurar a conexão com o local de rede para descoberta de pacotes. Portanto, (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html) com antecedência e certifique-se de que pelo menos um VDA no grupo atenda aos seguintes requisitos:

- Versão do VDA:
  - Para descobrir pacotes App-V: 2203 ou posterior
  - Para descobrir pacotes MSIX e MSIX app attach: 2209 ou posterior
- Componente Citrix Personalization for App-V: Instalado
- Permissão no local do pacote: Leitura (Consulte (#store-application-packages-on-network-shares) para obter detalhes.)
- Energia: Ligado
- Estado: Registrado

### Carregar pacotes de aplicativos em massa

Carregue pacotes em um local de rede para o seu ambiente. Certifique-se de ter os seguintes itens prontos antes do carregamento:

- Um grupo de entrega que atenda aos requisitos de (#preparations)
- O caminho do local de rede

Para carregar pacotes em massa, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Fontes**, clique no botão **Adicionar Fonte**. A página **Adicionar Fonte** é exibida.
3. No campo **Nome**, insira um nome descritivo para a fonte do pacote.
4. No campo **Grupo de entrega**, clique em **Selecionar um grupo de entrega**. Em seguida, selecione um grupo de entrega que atenda aos requisitos indicados em (#preparations) e clique em **OK**.
5. No campo **Tipo de local**, selecione **Servidor Microsoft App-V** ou **Compartilhamento de rede** com base em onde você armazena os pacotes e, em seguida, conclua as configurações correspondentes:
   - Se você selecionar **Servidor Microsoft App-V**, insira as seguintes informações:
     - URL do servidor de Gerenciamento. Exemplo: `http://appv-server.example.com`

    - Credenciais de login do administrador do servidor de gerenciamento.
    - URL e número da porta do servidor de publicação. Exemplo: `http://appv-server.example.com:3330`

- Se você selecionou **Compartilhamento de rede**, especifique as seguintes informações:
    - Insira o caminho UNC do compartilhamento de rede. Exemplo: `\\Package-Server\apps\`
    - Selecione os tipos de pacote que você deseja carregar. As opções incluem App-V, MSIX e MSIX app attach.
    - Especifique se deseja pesquisar subpastas por pacotes.

6. Clique em **Adicionar Fonte**.

   A página Adicionar Fonte é fechada e a fonte recém-adicionada aparece na lista de fontes. O Citrix Virtual Apps and Desktops carrega os pacotes para o seu ambiente usando um VDA no grupo de entrega. Após a conclusão do upload, o campo Status mostra *Importação bem-sucedida*. Os pacotes correspondentes aparecem na guia **Pacotes**.

> **Observação:**
>
> Para verificar se há atualizações de pacote em um local de origem e importá-las para o seu ambiente, selecione o local na lista de fontes e clique em **Verificar Atualizações de Pacote**.

### Carregar pacotes de aplicativos um por um

Carregue um pacote de aplicativo de um compartilhamento de rede para seu ambiente. Antes do upload, certifique-se de ter os seguintes itens prontos:

- Um grupo de entrega que atenda aos requisitos indicados em (#preparations)
- O caminho do local de rede.

Para carregar um pacote para seu ambiente, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Pacotes**, clique no botão **Adicionar pacote**. A página **Adicionar pacote** é exibida.

3. No campo **Grupo de entrega**, clique em **Selecionar um grupo de entrega**. Em seguida, selecione um grupo de entrega que atenda aos requisitos indicados em Preparação e clique em **OK**.
4. No campo **Caminho completo do pacote**, insira um caminho conforme necessário:
   - Para carregar vários pacotes de uma vez, insira seus caminhos completos, separados por ponto e vírgula ( `;` ). Exemplo: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Para carregar todos os pacotes presentes em um compartilhamento de rede, insira o caminho de armazenamento. Exemplo: `\\package-Server\apps\`
5. Clique em **Adicionar Pacote**.

   O pacote de aplicativos aparece na guia **Pacotes**.

### Adicionar aplicativos a grupos de entrega

Depois que um pacote de aplicativos for totalmente carregado, adicione seus aplicativos a um ou mais grupos de entrega, conforme necessário. Como resultado, os usuários associados a esses grupos de entrega podem acessar os aplicativos.

Para adicionar um ou mais aplicativos em um pacote a vários grupos de entrega, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Pacotes**, selecione um pacote conforme necessário.
3. Na barra de ações, clique em **Adicionar Grupos de Entrega**. A página Adicionar Grupos de Entrega é exibida.
4. Selecione um ou mais aplicativos no pacote, conforme necessário, e clique em **Avançar**. Grupos de entrega com o tipo de entrega *Aplicativos* são exibidos.
5. Na lista de grupos de entrega, selecione os grupos aos quais você deseja atribuir os aplicativos e clique em **Avançar**. **Nota:** Se você selecionou um pacote MSIX ou MSIX app attach, somente os grupos de entrega cujo nível funcional é 2106 ou posterior são mostrados na lista.
6. Clique em **Concluir**.

Você também pode adicionar aplicativos empacotados a um grupo de entrega quando:

- Criar um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.

- Editar grupos de entrega ou grupos de aplicativos existentes. Para obter mais informações, consulte Adicionar aplicativos.

### (Opcional) Criar grupos de isolamento para pacotes App-V

Você pode criar grupos de isolamento para permitir a entrega automática de pacotes App-V interdependentes.

> **Observação:**
>
> Grupos de isolamento são suportados para o método App-V Single Admin. Se você estiver usando o método App-V Dual Admin, poderá atingir o mesmo objetivo criando *grupos de conexão* na infraestrutura do Microsoft App-V. Para obter mais informações, consulte este artigo da documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/application-management/app-v/appv-connection-group-file>`.

#### Sobre grupos de isolamento

Um grupo de isolamento é uma coleção de pacotes de aplicativos interdependentes que devem ser executados na mesma Windows Sandbox para criar um ambiente virtual. Os grupos de isolamento do Citrix App-V são semelhantes, mas não idênticos, aos grupos de conexão do App-V. Um grupo de isolamento inclui dois tipos de pacotes:

- Pacotes de aplicativos **explícitos**. Aplicativos com requisitos de licenciamento específicos. Você pode restringir esses aplicativos a um intervalo específico de usuários, adicionando-os a grupos de entrega.
- Pacotes de aplicativos **automáticos**. Aplicativos que estão sempre disponíveis para todos os usuários, independentemente de serem adicionados a grupos de entrega.

Por exemplo, o aplicativo `app-a` requer JRE 1.7 para ser executado. Você pode criar um grupo de isolamento que contém app-a (marcado como *Explícito*) e JRE 1.7 (marcado como *Automático*). Em seguida, adicione o pacote App-V para `app-a` a um ou mais grupos de entrega. Quando um usuário inicia o app-a, o JRE 1.7 é implantado automaticamente com ele.

Quando um usuário inicia um aplicativo App-V marcado como *Explícito* em um grupo de isolamento, o Citrix Virtual Apps and Desktops verifica a permissão de acesso do usuário ao aplicativo em grupos de entrega. Se o usuário tiver permissão para acessar o aplicativo, quaisquer pacotes de aplicativos *Automáticos* no mesmo grupo de isolamento serão disponibilizados ao usuário.

Você não precisa adicionar os pacotes *Automáticos* a nenhum grupo de entrega. Se houver outro pacote de aplicativo *Explícito* no grupo de isolamento, esse pacote será disponibilizado ao usuário somente se estiver no mesmo grupo de entrega.

Para obter mais informações sobre grupos isolados, consulte este blog da Citrix.

#### CRIAR UM GRUPO DE ISOLAMENTO APP-V

Crie um grupo de isolamento e adicione pacotes de aplicativos interdependentes a ele. As etapas detalhadas são as seguintes:

1. Na guia **Grupos de Isolamento**, clique em **Adicionar Grupo de Isolamento**.
2. Insira um nome e uma descrição para o grupo de isolamento. Todos os pacotes de aplicativos em seu ambiente aparecem na lista **Pacotes Disponíveis**.
3. Na lista **Pacotes Disponíveis**, selecione um aplicativo conforme necessário e clique na seta para a direita. O aplicativo selecionado aparece na lista **Pacotes no Grupo de Isolamento**.
4. No campo **Implantação**, selecione **Explícito** ou **Automático** para o aplicativo.
5. Repita os passos 2–3 para adicionar mais pacotes.
6. Para ajustar a ordem dos pacotes na lista, clique na seta para cima ou para baixo.
7. Clique em **Salvar**.

> **Observação:**

> As configurações do Grupo de Isolamento resultam na criação de Grupos de Conexão App-V no VDA. Os cenários de implantação podem se tornar complexos e o cliente App-V suporta pacotes que estão em apenas um Grupo de Conexão ativo por vez. Recomendamos que você evite adicionar o mesmo pacote a dois grupos de isolamento diferentes que são adicionados ao mesmo grupo de entrega.

### Publicar aplicativos empacotados em VDAs de sessão única ou de desktop compartilhado

Agora você pode entregar pacotes App-V, MSIX e MSIX app attach para suas sessões VDA de sessão única ou de desktop compartilhado diretamente por meio de grupos de entrega. Você pode acessar os aplicativos empacotados em seu VDA de desktop no logon, com base nas permissões de acessibilidade definidas nos aplicativos.

### Benefícios

- Aplicativos disponíveis no VDA no logon e não preparados sob demanda via Workspace ou StoreFront.
- Tempo de inicialização aprimorado ao acessar os aplicativos empacotados.
- Facilita a manutenção dos aplicativos empacotados de forma independente, separadamente da imagem base do VDA.

### Considerações

- Esta opção está disponível para VDAs de sessão única apenas por meio do SDK do PowerShell apropriado. Atualmente, não está disponível no fluxo de trabalho do Web Studio. A publicação em desktops compartilhados pode ser feita com o SDK do PowerShell ou da maneira existente por meio do fluxo de trabalho do Web Studio. Para obter mais informações sobre o procedimento existente, consulte Adicionar aplicativos a grupos de entrega.
- Os aplicativos devem fazer parte de um grupo de entrega.

### Antes de começar

- Certifique-se de que os aplicativos empacotados estejam assinados e disponíveis no compartilhamento de arquivos ou local UNC. Para obter mais informações, consulte Armazenar pacotes de aplicativos em compartilhamentos de rede.
- Instale o componente de Personalização Citrix nas máquinas VDA.

### Procedimento

Para entregar aplicativos empacotados a VDAs de desktop, siga estas etapas:

1. Importar pacotes de aplicativos para o Web Studio.
2. Publicar o BrokerApplication empacotado.
3. Limitar a visibilidade dos aplicativos no Web Studio.

### Importar pacotes de aplicativos para o Web Studio

1. Abra um navegador da web. Digite `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Crie um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.
3. Importe os pacotes de aplicativos para o Web Studio. Para obter mais informações, consulte Carregar pacotes de aplicativos em massa.

### Publicar o aplicativo empacotado no BrokerApplication

Se você estiver publicando em um VDA multi-sessão (compartilhado) ou em um VDA de aplicativo de sessão única, o procedimento de publicação permanece inalterado. Para obter mais informações, consulte Adicionar aplicativos a grupos de entrega. Se você estiver publicando em um VDA de desktop de sessão única, faça o seguinte:

No Delivery Controller™, execute os seguintes comandos PowerShell:

1. Para recuperar os comandos presentes no pacote:

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **Observação:**
   >
   > A versão do `App-V package discovery module` que oferece suporte a essa funcionalidade pode ser encontrada no ISO do Citrix Virtual Apps and Desktops (versões 2311 ou superiores) no caminho acima.

2. Para recuperar os IDs de grupo de entrega e os IDs de aplicativos empacotados relevantes:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. Para publicar os pacotes e criar as BrokerMachineConfigurations apropriadas:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Para sincronizar as configurações do Broker, que são posteriormente enviadas para o agente Broker no VDA:

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>
   ```

   > **Observação:**
   >
   > Certifique-se de executar o comando PowerShell `Update-DesktopGroupMachineConfigurations` depois de publicar ou remover aplicativos empacotados de um VDA.

### Limitar a visibilidade de aplicativos no Web Studio

Por padrão, os usuários têm todos os aplicativos empacotados atribuídos ao grupo de entrega que atende ao seu VDA disponíveis em sua sessão de desktop. Você pode controlar a visibilidade de aplicativos empacotados nos VDAs de desktop definindo a visibilidade dos aplicativos para usuários ou grupos específicos no Web Studio. Para gerenciar a visibilidade de aplicativos empacotados, consulte Alterar Propriedades do Aplicativo.

## Aplicativos da Plataforma Universal do Windows

Para obter informações sobre aplicativos da Plataforma Universal do Windows (UWP), consulte a seguinte documentação da Microsoft:

- O que é um aplicativo da Plataforma Universal do Windows (UWP)?
- Gerenciador de Pacotes do Windows

### Requisitos e limitações

O Citrix Virtual Apps and Desktops™ oferece suporte ao uso de aplicativos UWP com VDAs nas seguintes máquinas Windows:

- Windows 10 e versões posteriores
- Windows Server 2016 e versões posteriores

Os VDAs devem ser no mínimo da versão 7.11.

Os seguintes recursos do Citrix Virtual Apps and Desktops não são suportados ou são limitados ao usar aplicativos UWP:

- A associação de tipo de arquivo não é suportada.
- O Acesso a Aplicativos Locais não é suportado.
- Visualização dinâmica: Se os aplicativos em execução na sessão se sobrepuserem, a visualização mostrará o ícone padrão. As APIs Win32 usadas para Visualização Dinâmica não são suportadas em aplicativos UWP.
- Remoting do Centro de Ações: Aplicativos UWP podem usar o Centro de Ações para exibir as mensagens na sessão. Essas mensagens atualmente não são redirecionadas para o endpoint para serem exibidas ao usuário.

O lançamento de aplicativos UWP e aplicativos não-UWP do mesmo servidor não é suportado. Em vez disso, coloque os aplicativos UWP e não-UWP em grupos de entrega ou grupos de aplicativos separados.

Como todos os aplicativos UWP instalados na máquina são enumerados, a Citrix® recomenda desabilitar o acesso do usuário à Windows Store. Isso impede que os aplicativos UWP instalados por um usuário sejam acessados por um usuário diferente.

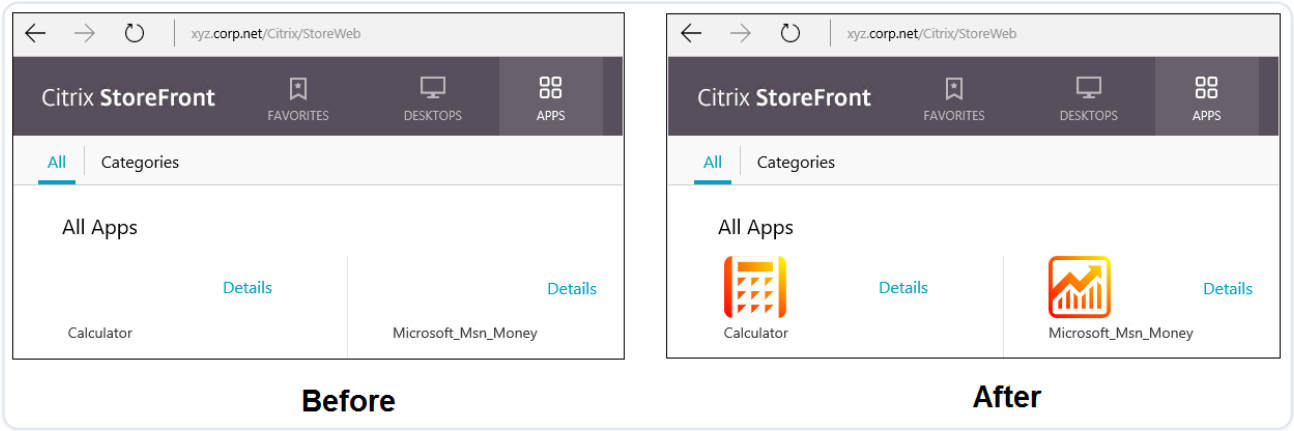
Durante o sideload, o aplicativo UWP é instalado na máquina e fica disponível para uso por outros usuários. Quando outro usuário inicia o aplicativo, ele é instalado e o sistema operacional atualiza seu banco de dados AppX para indicar "como instalado" por esse usuário.

Um logoff normal iniciado a partir de um aplicativo UWP publicado que foi iniciado em uma janela fixa ou contínua pode impedir que a sessão VDA seja encerrada e forçar o logoff do usuário. Quando isso ocorre, vários processos restantes na sessão VDA impedem que ela seja encerrada corretamente. Para resolver isso, determine qual processo está impedindo o encerramento da sessão VDA e, em seguida, adicione-o ao valor da chave de registro "LogoffCheckSysModules", seguindo as orientações em CTX891671.

Os nomes de exibição e as descrições dos aplicativos UWP podem não estar corretos. Edite e corrija essas propriedades ao adicionar os aplicativos ao grupo de entrega.

Verifique Problemas conhecidos para quaisquer problemas adicionais.

Atualmente, vários aplicativos UWP têm ícones brancos com transparência ativada, o que faz com que o ícone não seja visível contra o fundo branco da exibição do StoreFront. Para evitar esse problema, você pode alterar o plano de fundo. Por exemplo, na máquina StoreFront, edite o arquivo `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. No final do arquivo, adicione `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`. O gráfico a seguir ilustra o antes e o depois para este exemplo.




No Windows Server 2016 e versões posteriores, o Gerenciador do Servidor também pode ser iniciado quando um aplicativo UWP é iniciado. Para evitar que isso ocorra, você pode desabilitar o início automático do Gerenciador do Servidor durante o logon com a chave de registro `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Para obter

detalhes, consulte `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`.

### Instalar e publicar aplicativos UWP

O suporte para aplicativos UWP é habilitado por padrão.

Para instalar um ou mais aplicativos UWP em VDAs (ou uma imagem mestre), use um dos seguintes métodos:

- Conclua uma instalação offline da Windows Store for Business, usando uma ferramenta como o Deployment Image Servicing and Management (DISM) para implantar os aplicativos na imagem da área de trabalho. Para obter mais informações, consulte Windows Package Manager.
- Faça o sideload dos aplicativos. Para obter mais informações, consulte Sideload line of business (LOB) apps in Windows client devices.
- Instale os aplicativos UWP para cada usuário pretendido diretamente da Windows Store for Business.

Para adicionar (publicar) um ou mais aplicativos UWP no Citrix Virtual Apps ou Citrix Virtual Desktops™:

1. Depois que os aplicativos UWP são instalados na máquina, adicione os aplicativos UWP a um grupo de entrega ou grupo de aplicativos. Você pode fazer isso ao criar um grupo ou mais tarde. Na página **Aplicativos**, no menu **Adicionar**, selecione **Do menu Iniciar**.
2. Quando a lista de aplicativos aparecer, selecione os aplicativos UWP que você deseja publicar.
3. Continue com o assistente ou feche a caixa de diálogo de edição.

Para desabilitar o uso de Aplicativos Universais em um VDA, adicione a configuração de registro **EnableUWASeamlessSupport** em `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` e defina como **0**.

### Desinstalar aplicativos UWP

Quando você desinstala um aplicativo UWP com um comando como `Remove-AppXPackage`, o item é desinstalado apenas para administradores. Para remover o aplicativo das máquinas dos usuários que podem ter iniciado e usado o aplicativo, execute o comando de remoção em cada máquina. Você não pode desinstalar o pacote AppX das máquinas de todos os usuários com um único comando.

# Autoscale™

> **Nota:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este recurso está disponível apenas no Web Studio.

> O Autoscale é um recurso que fornece uma solução consistente e de alto desempenho para gerenciar proativamente o consumo de energia de suas máquinas. Ele visa equilibrar custos e experiência do usuário.

O Autoscale permite o gerenciamento proativo de energia de todas as máquinas OS de sessão única e multissessão registradas em um grupo de entrega.

Os recursos do Autoscale incluem:

- Configurações baseadas em agendamento e em carga
- Tempos limite de sessão dinâmicos
- Máquinas marcadas pelo Autoscale (burst de nuvem)
- Notificações de logoff do usuário

## Plataformas de hospedagem de VDA suportadas

O Autoscale oferece suporte a todas as plataformas que o Citrix Virtual Apps and Desktops oferece suporte. Isso inclui várias plataformas de infraestrutura, incluindo XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e muitas outras. Para obter uma lista completa de plataformas compatíveis, consulte Requisitos do sistema para Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Ao adicionar conexões de host de nuvem pública à sua implantação, você precisa da Licença de Direitos Híbridos. Para obter informações sobre a Licença de Direitos Híbridos, consulte Transição e Upgrade (TTU) com Direitos Híbridos. Para obter informações sobre como adicionar uma licença, consulte Criar um site.

## Cargas de trabalho suportadas

O Autoscale suporta grupos de entrega de SO multi-sessão e SO de sessão única. Existem três interfaces de usuário a serem consideradas:

- Interface de usuário do Autoscale para grupos de entrega de SO multi-sessão (anteriormente grupos de entrega RDS)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única aleatórios (agrupados) (anteriormente grupos de entrega VDI agrupados)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única estáticos (anteriormente grupos de entrega VDI estáticos)

Para obter mais informações sobre as interfaces de usuário para diferentes grupos de entrega, consulte Interfaces de usuário do Autoscale.

## Benefícios

O recurso Autoscale oferece os seguintes benefícios:

- Fornecer um mecanismo único e consistente para gerenciar o consumo de energia das máquinas em um grupo de entrega.
- Garantir a disponibilidade e controlar os custos, ligando as máquinas com gerenciamento de energia baseado em carga ou baseado em agendamento, ou uma combinação de ambos.
- Para monitorar métricas como economia de custos e utilização da capacidade, e para habilitar notificações, use Director.

## Assista a um vídeo de 2 minutos

O vídeo a seguir oferece um tour rápido pelo Autoscale.

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

## Introdução ao Autoscale™

O Autoscale funciona no nível do grupo de entrega. Ele gerencia proativamente a energia das máquinas em um grupo de entrega com base nos agendamentos que você define.

Autoscale aplica-se a todos os tipos de grupos de entrega:

- SO estático de sessão única
- SO aleatório de sessão única

- SO aleatório de múltiplas sessões

> **Nota:**
>
> O Autoscale é habilitado por padrão se você criar ou atualizar Grupos de Entrega usando o Studio baseado em MMC.

> Este artigo descreve conceitos básicos relacionados ao Autoscale e fornece orientações sobre como habilitar e configurar o Autoscale para um grupo de entrega.

## Conceitos básicos

Antes de começar, aprenda sobre os seguintes conceitos básicos no Autoscale:

- Agendamentos
- Buffer de capacidade
- Índice de carga

### Agendamentos

O Autoscale liga e desliga máquinas em um grupo de entrega com base em um agendamento que você define.

Um agendamento inclui o número de máquinas ativas para cada período, com horários de pico e fora de pico definidos.

As configurações de agendamento variam com o tipo de grupo de entrega. Para mais informações, consulte:

- Grupos de entrega de SO multi-sessão
- Grupos de entrega aleatórios de SO de sessão única
- Grupos de entrega estáticos de SO de sessão única

### Buffer de capacidade

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem considerados:

- Para grupos de entrega de SO multi-sessão, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga.

- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem do número total de máquinas no grupo de entrega.

### Índice de carga

> **IMPORTANTE:**

> O índice de carga se aplica apenas a grupos de entrega multi-sessão.

> A métrica do índice de carga determina a probabilidade de uma máquina receber solicitações de logon de usuário. Ela é calculada usando as configurações da **política de Gerenciamento de Carga do Citrix** configuradas para logon simultâneo, sessão, CPU, disco e uso de memória.

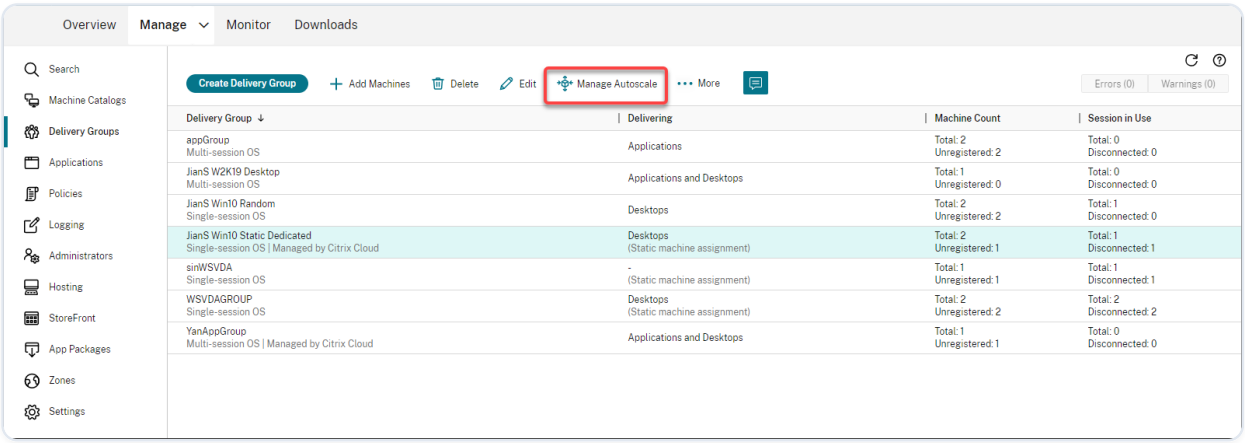
O índice de carga varia de 0 a 10.000. Por padrão, uma máquina é considerada em carga total quando hospeda 250 sessões:

- O dígito "0" indica uma máquina descarregada. Uma máquina com um valor de índice de carga de 0 está em uma carga de linha de base.
- O dígito "10.000" indica uma máquina totalmente carregada que não pode executar mais sessões.
- O dígito "10.000" indica uma máquina totalmente carregada que não pode executar mais nenhuma sessão.

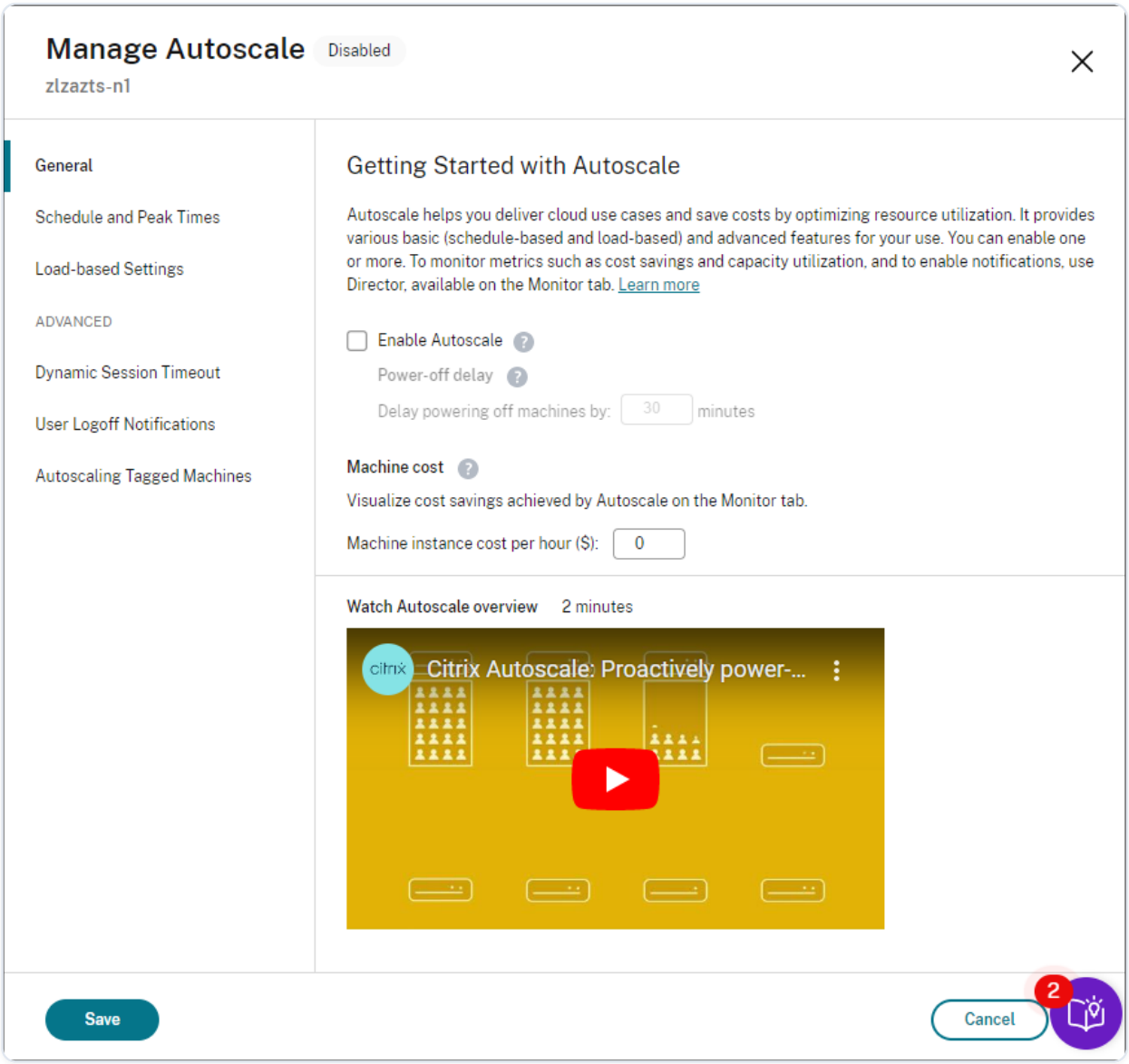
O Autoscale é desabilitado por padrão ao criar um grupo de entrega. Para habilitar e configurar o Autoscale para um grupo de entrega usando o Web Studio, siga estas etapas:

Você também pode usar comandos do PowerShell para habilitar e configurar o Autoscale para um grupo de entrega. Para obter mais informações, consulte comandos do SDK do PowerShell do Broker.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo de entrega que você deseja gerenciar e clique em **Gerenciar Autoscale**.




3. Na página **Gerenciar Autoscale**, selecione a caixa de seleção **Habilitar Autoscale** para habilitar o Autoscale. Depois de habilitar o Autoscale, as opções na página são habilitadas.




4. Para alterar as configurações padrão com base nas necessidades da sua organização, conclua as seguintes configurações:

- Configurar agendamentos
- Para desligar máquinas inativas de forma mais eficiente, use Tempos limite de sessão dinâmicos e Notificações de logoff do usuário
- Para gerenciar o consumo de energia de um subconjunto de máquinas no grupo de entrega, use Máquinas marcadas com dimensionamento automático

Para desabilitar o Autoscale, desmarque a caixa de seleção **Autoscale**. As opções na página ficam cinzas para indicar que o Autoscale está desabilitado para o grupo de entrega selecionado.

> **Importante:**
>
> - Se você desabilitar o Autoscale, todas as máquinas gerenciadas pelo Autoscale permanecem em seus estados no momento da desabilitação.
> - Depois de desabilitar o Autoscale, as máquinas em estado de drenagem são retiradas do estado de drenagem. Para obter mais informações sobre o estado de drenagem, consulte Estado de drenagem.

### Monitorar métricas

Depois de habilitar o Autoscale para um grupo de entrega, você pode monitorar as seguintes métricas de máquinas gerenciadas pelo Autoscale a partir do Director.

- Uso da máquina
- Economia estimada
- Notificações de alerta para máquinas e sessões
- Status da máquina
- Tendências de avaliação de carga

> **Nota:**
>
> Quando você habilita o Autoscale inicialmente para um grupo de entrega, pode levar alguns minutos para exibir os dados de monitoramento desse grupo de entrega. Os dados de monitoramento permanecem disponíveis se o Autoscale for habilitado e depois desabilitado para o grupo de entrega. O Autoscale coleta dados de monitoramento em intervalos de 5 minutos.

> Para obter mais informações sobre as métricas, consulte Monitorar máquinas gerenciadas pelo Autoscale.

## É bom saber

O Autoscale funciona no nível do grupo de entrega. Ele é configurado por grupo de entrega. Ele gerencia o consumo de energia apenas das máquinas no grupo de entrega selecionado.

### Capacidade e registro de máquinas

O Autoscale inclui apenas máquinas que estão registradas no site ao determinar a capacidade. Máquinas ligadas que não estão registradas não podem aceitar solicitações de sessão. Como resultado, elas não são incluídas na capacidade geral do grupo de entrega.

### Dimensionamento entre vários catálogos de máquinas

Em alguns sites, vários catálogos de máquinas podem estar associados a um único grupo de entrega. O Autoscale liga máquinas aleatoriamente de cada catálogo para atender aos requisitos de agendamento ou demanda de sessão.

Por exemplo, um grupo de entrega tem dois catálogos de máquinas: o Catálogo A tem três máquinas ligadas e o Catálogo B tem uma máquina ligada. Se o Autoscale precisar ligar uma máquina extra, ele poderá ligar uma máquina do Catálogo A ou do Catálogo B.

### Provisionamento de máquinas e demanda de sessão

O catálogo de máquinas associado ao grupo de entrega deve ter máquinas suficientes para ligar e desligar conforme a demanda aumenta e diminui. Se a demanda de sessão exceder o número total de máquinas registradas no grupo de entrega, o Autoscale garante que todas as máquinas registradas sejam ligadas. No entanto, **o Autoscale não provisiona máquinas adicionais**.

### Considerações sobre o tamanho da instância

Você pode otimizar seus custos se dimensionar adequadamente suas instâncias em nuvens públicas. Recomendamos que você provisione instâncias menores, desde que elas correspondam ao desempenho da sua carga de trabalho e aos requisitos de capacidade.

Instâncias menores hospedam menos sessões de usuário do que instâncias maiores. Portanto, o Autoscale coloca as máquinas em estado de drenagem muito mais rapidamente porque leva menos tempo para que a última sessão de usuário seja desconectada. Como resultado, o Autoscale desliga instâncias menores mais cedo, reduzindo assim os custos.

### Estado de dreno

O Autoscale tenta reduzir o número de máquinas ligadas no grupo de entrega para o tamanho do pool configurado e o buffer de capacidade.

Para atingir esse objetivo, o Autoscale coloca as máquinas em excesso com o menor número de sessões em "estado de drenagem" e as desliga quando todas as sessões são encerradas. Esse comportamento ocorre quando a demanda por sessões diminui e o agendamento exige menos máquinas do que as que estão ligadas.

O Autoscale coloca máquinas em excesso em "estado de drenagem" uma a uma:

- Se duas ou mais máquinas tiverem o mesmo número de sessões ativas, o Autoscale drena a máquina que esteve ligada pelo atraso de desligamento especificado.

  Fazer isso evita colocar máquinas recém-ligadas em estado de drenagem, pois essas máquinas são mais propensas a ter o menor número de sessões.
- Se duas ou mais máquinas estiveram ligadas pelo atraso de desligamento especificado, o Autoscale drena essas máquinas uma a uma aleatoriamente.

Máquinas em estado de drenagem não hospedam mais novos inícios de sessão e estão aguardando que as sessões existentes sejam encerradas. Uma máquina se torna candidata a desligamento somente quando todas as sessões são encerradas. No entanto, se não houver máquinas imediatamente disponíveis para inícios de sessão, o Autoscale prefere direcionar os inícios de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina.

Uma máquina é retirada do estado de drenagem quando uma das seguintes condições é atendida:

- A máquina é desligada.
- O Autoscale está desabilitado para o grupo de entrega ao qual a máquina pertence.
- O Autoscale usa a máquina para atender aos requisitos de agendamento ou demanda de carga. Este caso ocorre quando o agendamento (escalonamento baseado em agendamento) ou a demanda atual (escalonamento baseado em carga) exige mais máquinas do que o número de máquinas atualmente ligadas.

> **Importante:**

> Se nenhuma máquina estiver imediatamente disponível para inicialização de sessões, o Autoscale prefere direcionar as inicializações de sessões para uma máquina em estado de

drenagem em vez de ligar uma máquina. Uma máquina em estado de drenagem que hospeda uma inicialização de sessão permanece em estado de drenagem.

Para descobrir quais máquinas estão em estado de drenagem, use o comando PowerShell `Get-BrokerMachine`. Por exemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternativamente, você pode usar o console Gerenciar. Consulte Exibir máquinas em estado de drenagem.

### EXIBIR MÁQUINAS EM ESTADO DE DRENAGEM

**Nota:**

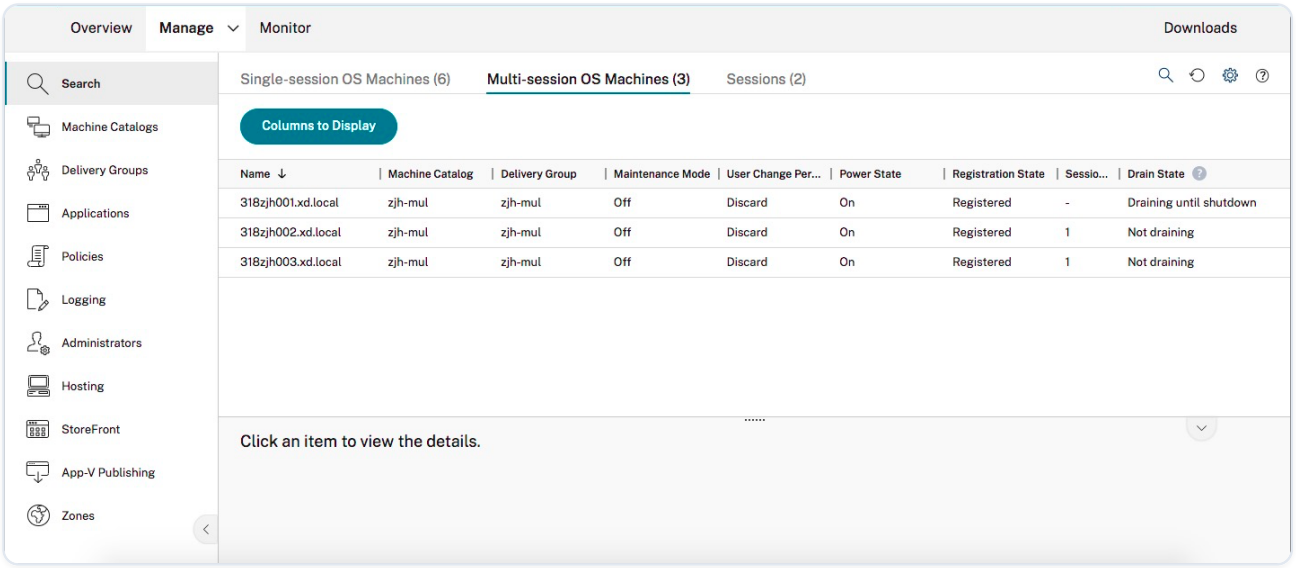
Este recurso se aplica apenas a máquinas de várias sessões.

No Web Studio, você pode exibir as máquinas que estão em estado de drenagem, informando quais máquinas estão prestes a ser desligadas. Conclua as seguintes etapas:

1. navegar para o nó **Pesquisar** e, em seguida, clique em **Colunas a Exibir**.
2. Na janela **Colunas a Exibir**, selecione a caixa de seleção ao lado de **Estado de Drenagem**.
3. Clique em **Salvar** para sair da janela **Colunas a Exibir**.

A coluna **Estado de Esgotamento** pode exibir as seguintes informações:

- **Drenando até o desligamento.** Aparece quando as máquinas estão no estado de drenagem até serem desligadas.
- **Não drenando.** Aparece quando as máquinas ainda não estão no estado de drenagem.




### Mais informações

Para obter mais informações sobre o Autoscale, consulte Citrix Autoscale na Tech Zone.

## Configurações baseadas em agendamento e baseadas em carga

### Como o Autoscale™ gerencia a energia das máquinas

O Autoscale liga e desliga as máquinas com base no agendamento selecionado. O Autoscale permite que você defina vários agendamentos que incluem dias específicos da semana e ajuste o número de máquinas disponíveis durante esses horários. Se você espera que um conjunto de usuários consuma os recursos da máquina em um horário específico em dias específicos, o Autoscale ajuda a fornecer uma experiência otimizada. Observe que essas máquinas serão ligadas durante o agendamento, independentemente de haver sessões em execução nelas.

> **Nota:**
>
> O Autoscale oferece suporte a qualquer máquina com gerenciamento de energia.

> O agendamento é baseado no **fuso horário** do grupo de entrega. Para alterar o fuso horário, você pode alterar as configurações do usuário em um grupo de entrega. Para obter mais informações, consulte Gerenciar Grupos de Entrega.

O Autoscale tem dois agendamentos padrão: *Dias da semana* (de segunda a sexta-feira) e *Fim de semana* (sábado e domingo). Por padrão, o agendamento de **Dias da semana** mantém uma máquina ligada das 07:00 às 18:30 durante os horários de pico e nenhuma durante os horários de menor movimento. O buffer de capacidade padrão é definido como 10% durante os horários de

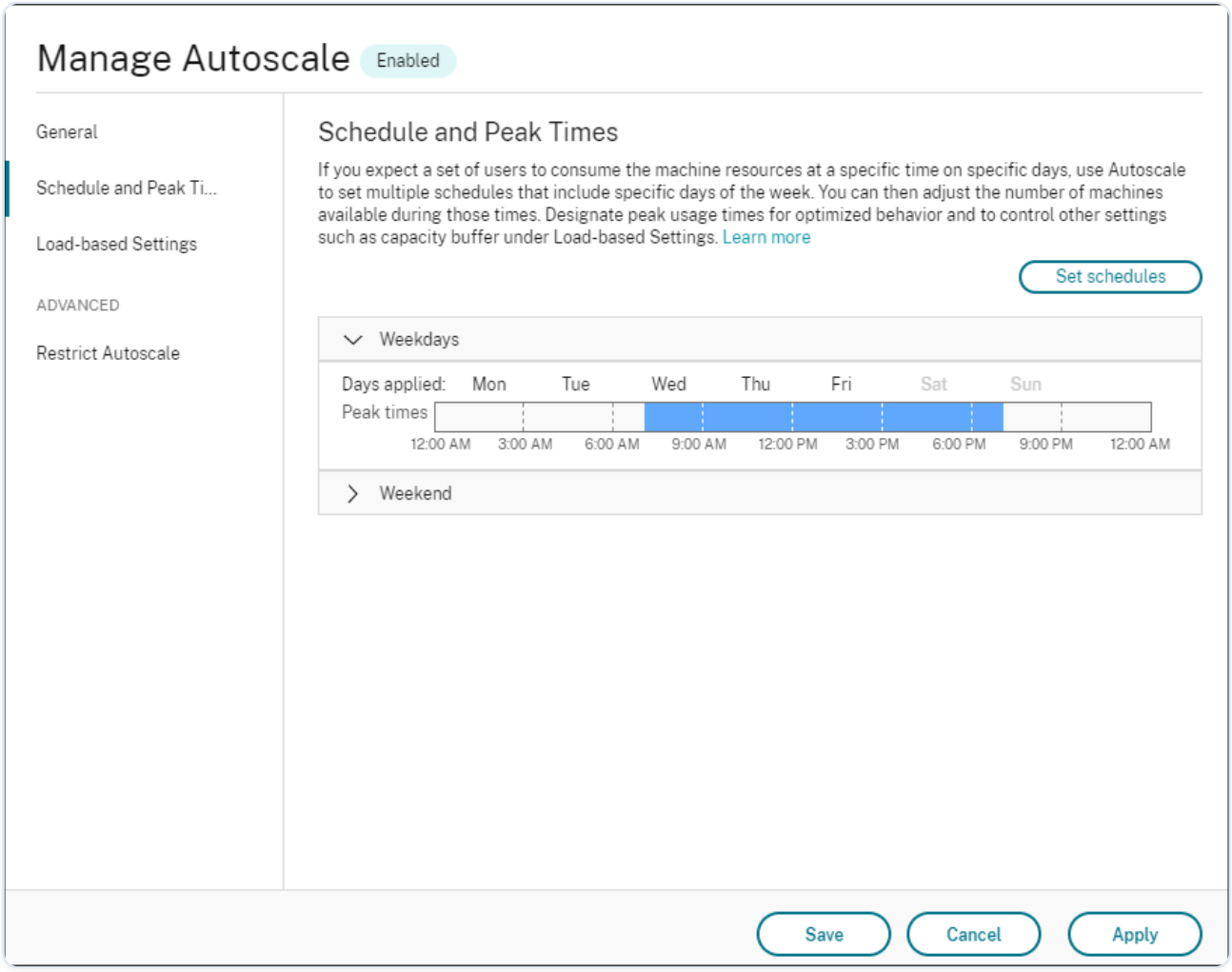
pico e de menor movimento. Por padrão, o agendamento de **Fim de semana** não mantém nenhuma máquina ligada.

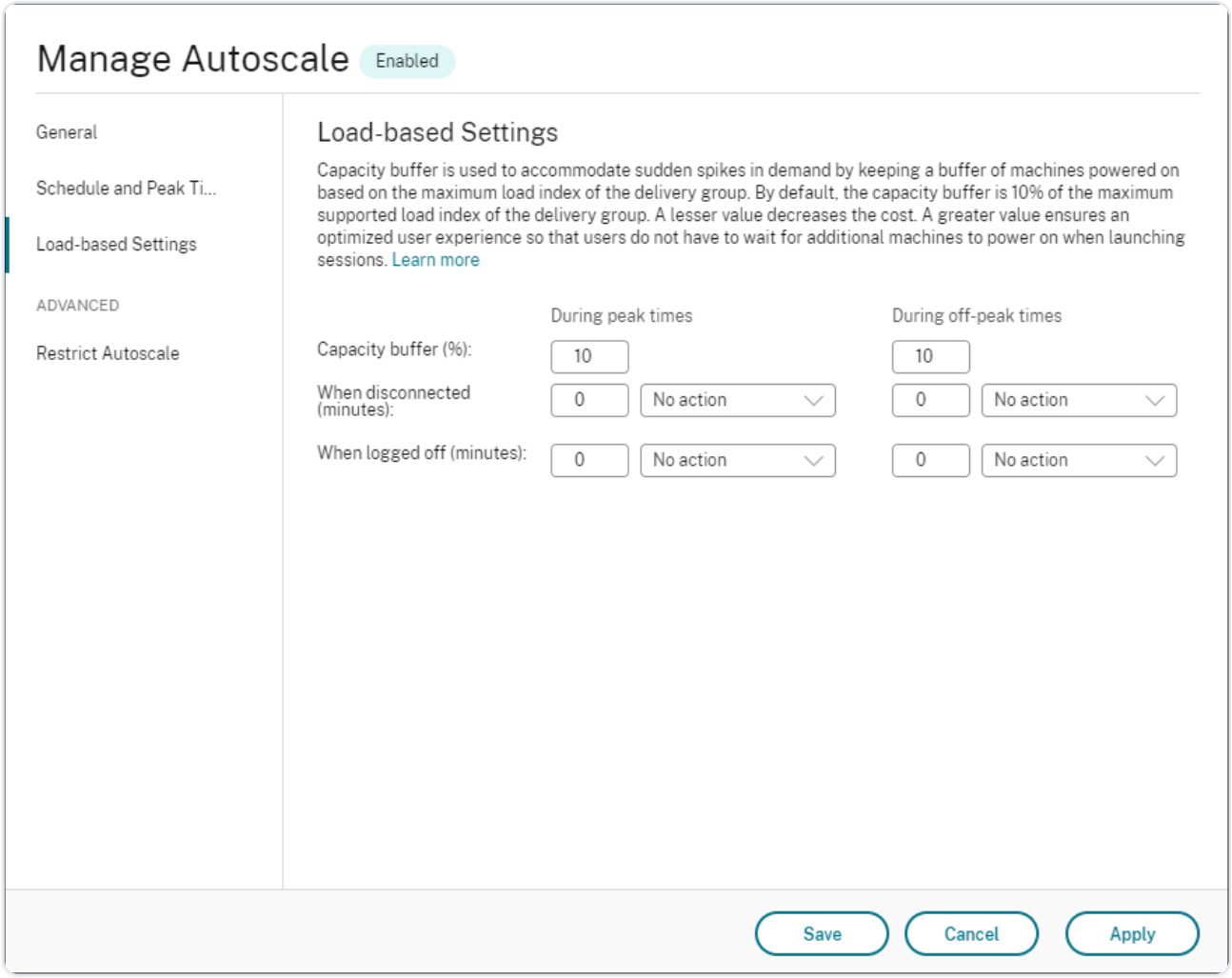
> **Nota:**
>
> O Autoscale considera apenas as máquinas registradas no site como parte da capacidade disponível nos cálculos que ele faz. "Registrada" significa que a máquina está disponível para uso ou já está em uso. Isso garante que apenas as máquinas que podem aceitar sessões de usuário sejam incluídas na capacidade do grupo de entrega.

### Interfaces de usuário

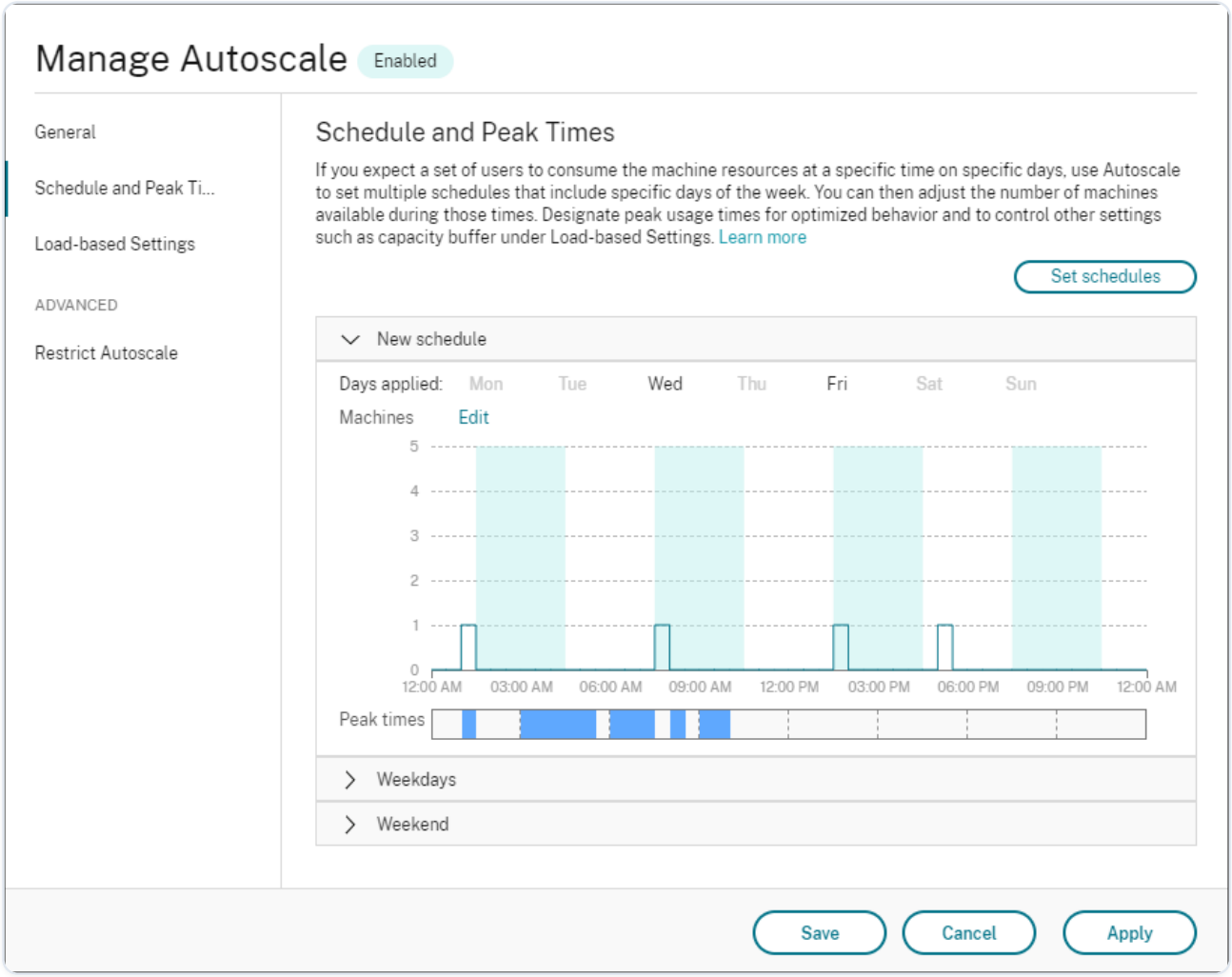
Existem três tipos de interfaces de usuário a serem consideradas.

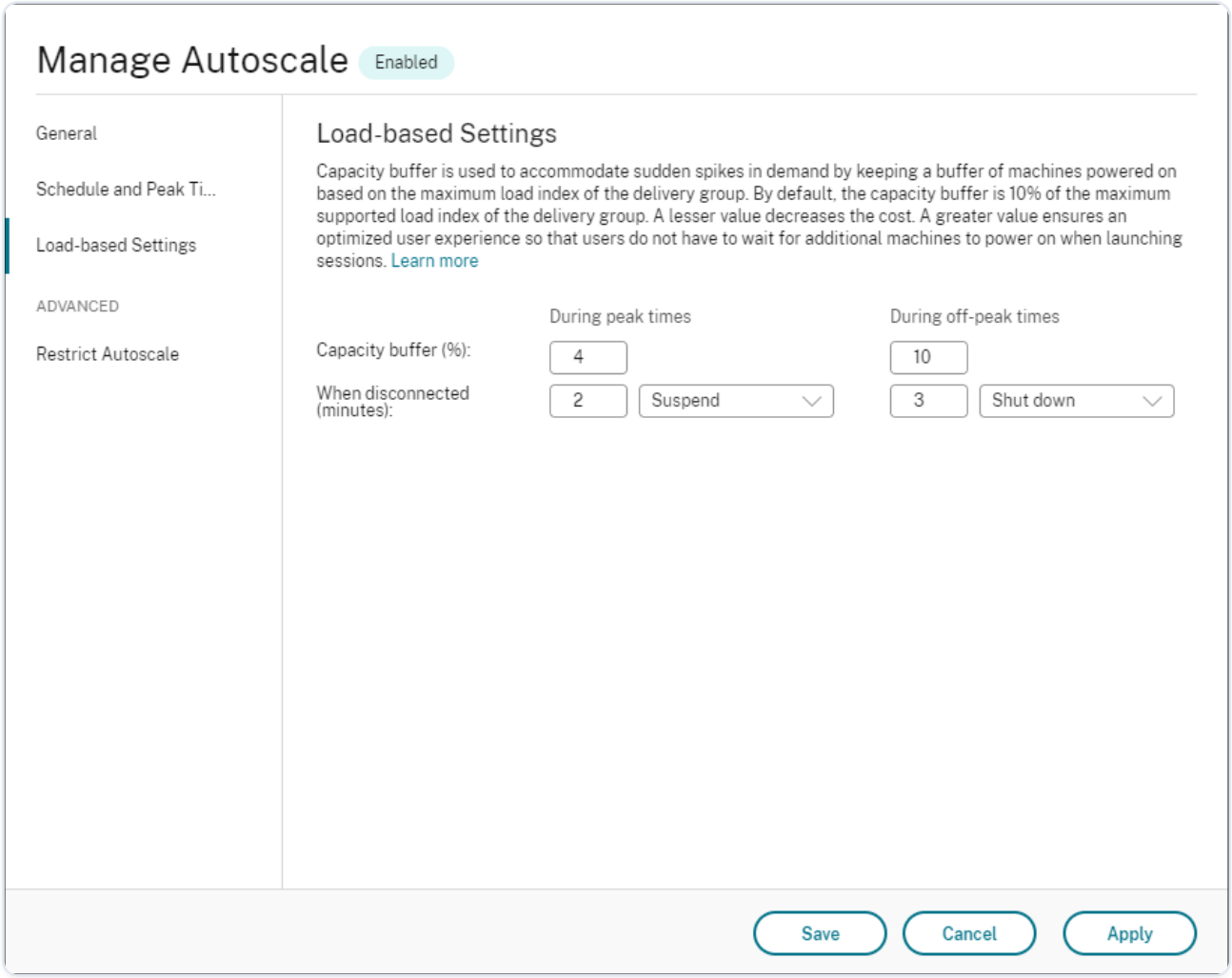
Interface de usuário para *grupos de entrega estáticos de SO de sessão única*:



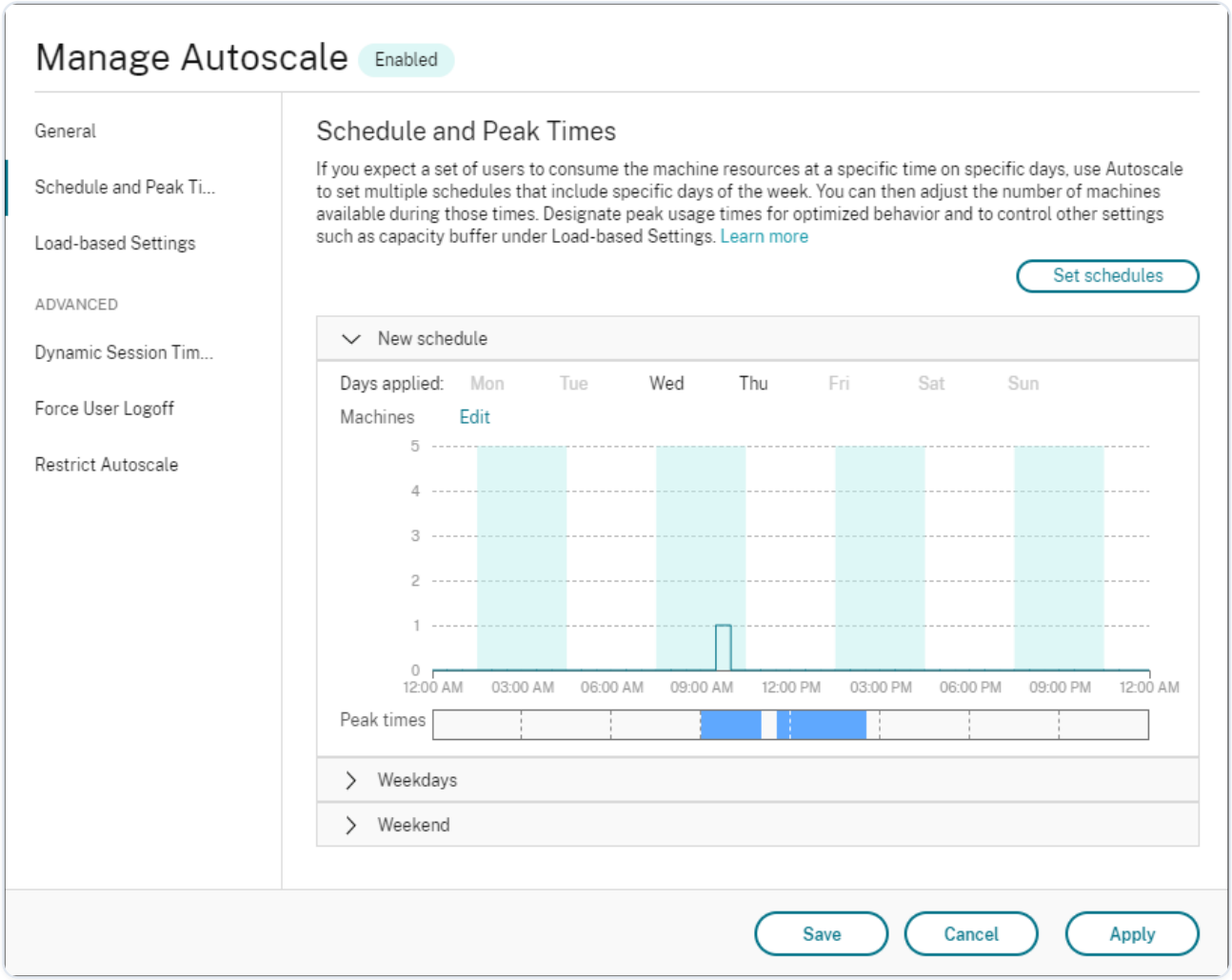


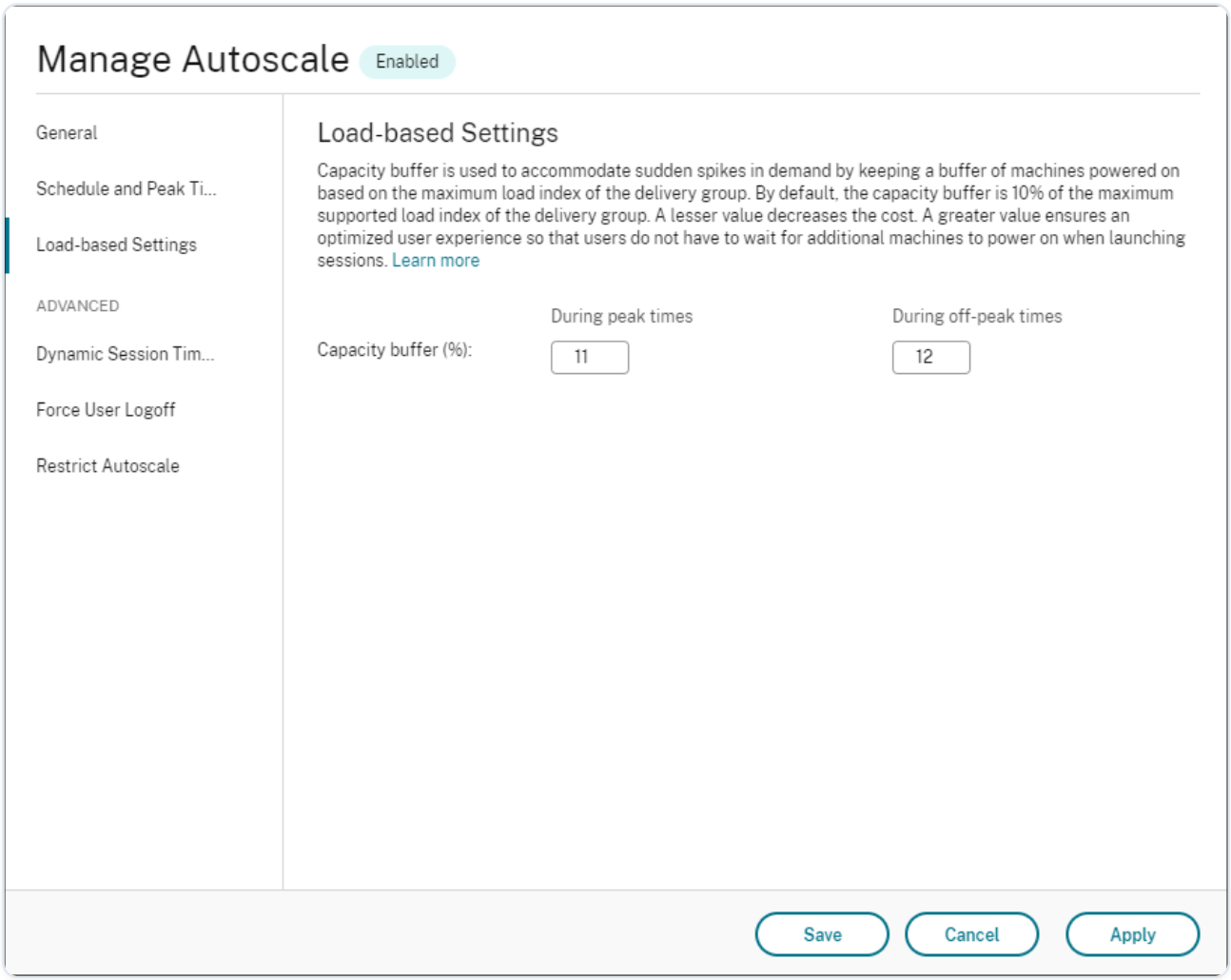

Interface de usuário do Autoscale para *grupos de entrega aleatórios de SO de sessão única*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply




Interface de usuário do Autoscale para *grupos de entrega de SO multi-sessão*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply




### Configurações baseadas em agendamento

**Agendamento do Autoscale**. Permite adicionar, editar, selecionar e excluir agendamentos.

**Dias aplicados**. Destaca os dias que você aplicou ao agendamento selecionado. Os dias restantes ficam esmaecidos.

**Editar**. Permite atribuir as máquinas a cada hora ou a cada meia hora. Você pode atribuir as máquinas por números e por porcentagens.

**Nota:**

- Esta opção está disponível apenas nas interfaces de usuário do Autoscale para SO multi-sessão e grupos de entrega aleatórios de SO de sessão única.
- O histograma ao lado de **Editar** exibe o número ou a porcentagem de máquinas que estão em execução em diferentes intervalos de tempo.

- Você pode **atribuir máquinas** a cada intervalo de tempo clicando em **Editar** acima de **Horários de pico**. Dependendo da opção selecionada no menu na janela **Máquinas para iniciar**, você pode atribuir as máquinas por números ou por porcentagens.
- Para grupos de entrega de SO multi-sessão, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 30 minutos durante cada dia. Para grupos de entrega aleatórios de SO de sessão única, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 60 minutos durante cada dia.

Para definir seus próprios agendamentos, siga estas etapas:

1. Na página **Agendamento e Horários de Pico** da janela **Gerenciar Autoscale**, clique em **Definir agendamentos**.
2. Na janela **Editar Agendamentos do Autoscale**, selecione os dias que deseja aplicar a cada agendamento. Você também pode excluir agendamentos, conforme aplicável.
3. Clique em **Concluído** para salvar os agendamentos e retornar à página **Agendamento e Horários de Pico**.
4. Selecione o agendamento aplicável e configure-o conforme necessário.
5. Clique em **Aplicar** para sair da janela **Gerenciar Autoscale** ou configurar as definições em outras páginas.

**Importante:**

- O Autoscale não permite que o mesmo dia se sobreponha em agendamentos diferentes. Por exemplo, se você selecionar segunda-feira no agendamento2 depois de selecionar segunda-feira no agendamento1, a segunda-feira será automaticamente desmarcada no agendamento1.
- Um nome de agendamento não diferencia maiúsculas de minúsculas.
- Um nome de agendamento não deve estar em branco ou conter apenas espaços.
- O Autoscale permite espaços em branco entre caracteres.
- Um nome de agendamento não deve conter os seguintes caracteres: \ / ; : # . * ? = < > \| ( ) { } " ' `.

- O Autoscale não oferece suporte a nomes de agendamento duplicados. Insira um nome diferente para cada agendamento.
- O Autoscale não oferece suporte a agendamentos vazios. Isso significa que os agendamentos sem dias selecionados não são salvos.

**Nota:**

Os dias incluídos no agendamento selecionado são destacados, enquanto os não incluídos são esmaecidos.

### Configurações baseadas em carga

**Horários de pico**. Permite definir os horários de pico para os dias aplicados no agendamento selecionado. Você pode fazer isso clicando com o botão direito do mouse no gráfico de barras horizontal. Depois de definir os horários de pico, os horários restantes e não definidos são padronizados para horários fora de pico. Por **padrão**, o período das 7:00 AM às 7:00 PM é definido como horários de pico para os dias incluídos no agendamento selecionado.

**Importante:**

- Para grupos de entrega de SO multi-sessão, o gráfico de barras de horários de pico é usado para o buffer de capacidade.
- Para grupos de entrega de SO de sessão única, o gráfico de barras de horários de pico é usado para o buffer de capacidade e controla as ações a serem acionadas após o logoff e/ou desconexão.
- Você pode definir os horários de pico para os dias incluídos em um agendamento em um nível granular de 30 minutos para grupos de entrega de SO de várias sessões e de sessão única. Alternativamente, você pode usar o comando `New-BrokerPowerTimeScheme PowerShell`. Para obter mais informações, consulte comandos do SDK do Broker PowerShell.

**Buffer de capacidade**. Permite manter um buffer de máquinas ligadas. Um valor menor diminui o custo. Um valor maior garante uma experiência de usuário otimizada para que, ao iniciar sessões, os usuários não precisem esperar que máquinas adicionais sejam ligadas.

Por padrão, o buffer de capacidade é de 10% para horários de pico e fora de pico. Se você definir o buffer de capacidade como 0 (zero), os usuários podem ter que esperar que máquinas adicionais sejam ligadas ao iniciar sessões. O Autoscale permite que você determine o buffer de capacidade separadamente para horários de pico e fora de pico.

### Configurações diversas

**Dica:**

- Você pode optar por configurar as configurações diversas usando o SDK do Broker PowerShell. Para obter mais informações, consulte comandos do SDK do Broker PowerShell.
- Para entender os comandos do SDK associados às configurações quando desconectado e quando o logoff é feito, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`.

**Quando desconectado**. Permite especificar por quanto tempo uma máquina desconectada e bloqueada permanece ligada após a desconexão da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de desconexão especificado expira, dependendo da ação configurada. Por padrão, nenhuma ação é atribuída a máquinas desconectadas. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina permanece ligada após a desconexão da sessão. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de desconexão especificado expira. A seguinte opção fica disponível depois que você seleciona **Suspender**.
    - **Quando não há reconexão em (minutos)**. Máquinas suspensas permanecem disponíveis para usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Para tornar as máquinas disponíveis novamente para manipular todas as cargas de trabalho, desligue-as. Especifique o tempo limite, em minutos, após o qual o Autoscale as desliga.

- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de desconexão especificado expira.

**Nota:**

Esta opção está disponível apenas nas interfaces de usuário do Autoscale para grupos de entrega de SO de sessão única aleatórios e estáticos.

**Quando o logoff é feito**. Permite especificar por quanto tempo uma máquina permanece ligada após o logoff da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de logoff especificado expira, dependendo das ações configuradas. Por padrão, nenhuma ação é atribuída a máquinas com logoff feito. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina permanece ligada após o logoff da sessão. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de logoff especificado expira.
- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de logoff especificado expira.

**Nota:**

Esta opção está disponível apenas na interface de usuário do Autoscale para grupos de entrega de SO de sessão única estáticos.

**Gerenciar energia de máquinas de SO de sessão única em transição para um período de tempo diferente com sessões desconectadas**

**Importante:**

- Este aprimoramento se aplica apenas a máquinas de SO de sessão única com sessões desconectadas. Não se aplica a máquinas de SO de sessão única com sessões encerradas.
- Para que este aprimoramento entre em vigor, você precisa habilitar o Autoscale para o grupo de entrega aplicável. Caso contrário, as ações da política de energia de desconexão não são acionadas na transição de período.

Em versões anteriores, uma máquina de SO de sessão única em transição para um período de tempo onde uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Este cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) onde nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir desta versão, o Autoscale suspende ou desliga a máquina quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega de SO de sessão única:

- Defina `PeakDisconnectAction` como "Nada"
- Defina `OffPeakDisconnectAction` como "Desligar"
- Defina 'OffPeakDisconnectTimeout' como "10"

**Nota:**

Para obter mais informações sobre a política de energia de ação de desconexão, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` e `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

Em versões anteriores, uma máquina de SO de sessão única com uma sessão desconectada durante os horários de pico permanecia ligada ao fazer a transição do pico para fora do pico. A partir desta versão, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina de SO de sessão única na

> transição de período. Como resultado, a máquina é desligada 10 minutos após a transição para fora do pico.

Caso você queira reverter para o comportamento anterior (ou seja, não tomar nenhuma ação em máquinas que fazem a transição do pico para fora do pico ou do fora do pico para o pico com sessões desconectadas), faça uma das seguintes opções:

- Defina o valor do registro "LegacyPeakTransitionDisconnectedBehaviour" como 1 (verdadeiro; habilita o comportamento anterior). Por padrão, o valor é 0 (falso; aciona ações da política de energia de desconexão na transição de período).
  - Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dados: 0x00000001 (1)
- Configure a configuração usando o `Set-BrokerServiceConfigurationData` comando PowerShell. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações da política de energia possam ser aplicadas a ela na transição de período:

- Tem uma sessão desconectada.
- Não tem ações de energia pendentes.
- Pertence a um grupo de entrega de SO de sessão única que faz a transição para um período de tempo diferente.
- Tem uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e faz a transição para um período onde uma ação de energia é atribuída.

### Como funciona o buffer de capacidade

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem observados:

- Para grupos de entrega de SO de várias sessões, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga. Para obter mais informações sobre o índice de carga, consulte Load index.
- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos do número de máquinas.

**Nota:**

Em cenários onde você restringe o Autoscale a máquinas marcadas, o buffer de capacidade é definido como uma porcentagem da capacidade total das máquinas marcadas no grupo de entrega em termos de índice de carga.

O Autoscale permite definir o buffer de capacidade separadamente para horários de pico e fora de pico. Um valor menor no campo do buffer de capacidade diminui o custo porque o Autoscale liga menos capacidade sobressalente. Um valor maior garante uma experiência de usuário otimizada para que os usuários não precisem esperar que máquinas adicionais sejam ligadas ao iniciar sessões. Por padrão, o buffer de capacidade é de 10%.

**Importante:**

O buffer de capacidade resulta em máquinas sendo ligadas quando a capacidade sobressalente total cai para um nível abaixo de "X" por cento da capacidade total do grupo de entrega. Ao fazer isso, a porcentagem necessária de capacidade sobressalente é reservada.

### Grupos de entrega de SO de várias sessões

#### Quando as máquinas são ligadas?

**Importante:**

Se um agendamento for selecionado, o Autoscale liga todas as máquinas configuradas para serem ligadas no agendamento. O Autoscale mantém esse número especificado de máquinas ligadas durante o agendamento, independentemente da carga.

Quando o número de máquinas ligadas no grupo de entrega não consegue mais atender ao buffer necessário para honrar a capacidade do buffer em termos de índice de carga, o Autoscale liga máquinas extras. Por exemplo, digamos que seu grupo de entrega tenha 20 máquinas e 3 máquinas estejam agendadas para serem ligadas como parte do dimensionamento baseado em agendamento com um buffer de capacidade de 20%. Eventualmente, 4 máquinas serão ligadas quando não houver carga. Isso ocorre porque um índice de carga de 4 x 10k é necessário como buffer; portanto, pelo menos 4 máquinas precisam ser ligadas. Este caso pode ocorrer durante horários de pico, aumento da carga nas máquinas, novos inícios de sessão e quando você adiciona novas máquinas ao grupo de entrega. Observe que o Autoscale liga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas não estão em modo de manutenção.
- O hipervisor no qual as máquinas estão sendo executadas não está em modo de manutenção.
- As máquinas estão atualmente desligadas.
- As máquinas não têm ações de energia pendentes.

**Quando as máquinas são desligadas?**

**Importante:**

- Se um agendamento for selecionado, o Autoscale desliga as máquinas com base no agendamento.
- O Autoscale não desliga as máquinas configuradas no agendamento para serem ligadas durante o agendamento.

Quando há máquinas mais do que suficientes para suportar o número alvo de máquinas ligadas (incluindo o buffer) para o grupo de entrega, o Autoscale desliga máquinas extras. Este caso pode ocorrer durante horários de baixa demanda, diminuição da carga nas máquinas e logoffs de sessão, e quando você remove máquinas do grupo de entrega. O Autoscale desliga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas e o hipervisor no qual as máquinas estão sendo executadas não estão em modo de manutenção.
- As máquinas estão atualmente ligadas.

- As máquinas são registradas como disponíveis ou aguardando registro após a inicialização.
- As máquinas não têm sessões ativas.
- As máquinas não têm ações de energia pendentes.
- As máquinas satisfazem o atraso de desligamento especificado. Isso significa que as máquinas estiveram ligadas por pelo menos "X" minutos, onde "X" é o atraso de desligamento especificado para o grupo de entrega.

### Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Sem carga de usuário (estado inicial)
  - Uma máquina (por exemplo, M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina é ligada.
  - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base (o índice de carga é igual a 0).
- O primeiro usuário faz logon

    - A sessão é direcionada para ser hospedada na máquina M1.
    - O índice de carga da máquina M1 ligada aumenta e a máquina M1 não está mais em uma carga de linha de base.
    - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.
    - O valor do índice de carga da máquina M2 está em uma carga de linha de base.
- Usuários aumentam a carga
    - As sessões são balanceadas entre as máquinas M1 e M2. Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta.
    - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
    - O valor do índice de carga da máquina M2 não está mais em uma carga de linha de base.
- Mais sessões de usuário são iniciadas
    - As sessões são balanceadas entre as máquinas (M1 e M2). Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta ainda mais.
    - Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.
    - O valor do índice de carga da máquina M3 está em uma carga de linha de base.
- Ainda mais sessões de usuário são iniciadas
    - As sessões são balanceadas entre as máquinas (M1 a M3). Como resultado, o índice de carga das máquinas ligadas (M1 a M3) aumenta.
    - A capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
    - O valor do índice de carga da máquina M3 não está mais em uma carga de linha de base.
- A carga da sessão do usuário diminui devido ao encerramento da sessão
    - Depois que os usuários saem de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M3 é reutilizada para hospedar sessões iniciadas por outros usuários.

    - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M3) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina, a menos que novas alterações ocorram. Por exemplo, a carga do usuário final aumenta novamente ou outras máquinas se tornam menos carregadas.

- A carga da sessão do usuário continua a diminuir
    - Depois que todas as sessões na máquina M3 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M3.
    - Depois que mais usuários encerram suas sessões, a capacidade liberada nas máquinas ligadas (M1 e M2) é reutilizada para hospedar sessões iniciadas por outros usuários.
    - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M2) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina.
- A carga da sessão do usuário continua a diminuir até que não haja sessões
    - Depois que todas as sessões na máquina M2 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M2.
    - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base. O Autoscale não coloca a máquina M1 no estado de esvaziamento devido ao buffer de capacidade configurado.

**Nota:**

Para grupos de entrega de SO multi-sessão, todas as alterações na área de trabalho são perdidas quando os usuários encerram as sessões. No entanto, se configurado, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

### Grupos de entrega aleatórios de SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas ligadas com base no número total de máquinas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas no grupo de entrega.

Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

### Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade é definido como 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Consulte abaixo para obter detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - Uma máquina (M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10% (buffer de capacidade configurado) é igual a 1. Portanto, uma máquina é ligada.
- Um primeiro usuário faz logon
  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas ligadas. Neste caso, o usuário recebe um desktop da máquina M1.
  - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.

- Um segundo usuário faz logon
  - O usuário recebe um desktop da máquina M2.
  - O Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.
- Um terceiro usuário faz logon
  - O usuário recebe um desktop da máquina M3.
  - O Autoscale começa a ligar uma máquina adicional (M4) para atender à demanda devido ao buffer de capacidade configurado.
- Um usuário faz logoff
  - Depois que um usuário faz logoff ou o desktop do usuário expira, a capacidade liberada (por exemplo, M3) fica disponível como buffer. Como resultado, o Autoscale começa a desligar a máquina M4 porque o buffer de capacidade está configurado para 10%.
- Mais usuários fazem logoff até que não haja mais usuários
  - Depois que mais usuários fazem logoff, o Autoscale desliga as máquinas (por exemplo, M2 ou M3).
  - Mesmo que não haja mais usuários, o Autoscale não desliga a máquina restante (por exemplo, M1) porque essa máquina está reservada como capacidade sobressalente.

> **Nota:**
>
> Para grupos de entrega aleatórios de SO de sessão única, todas as alterações na área de trabalho são perdidas quando os usuários encerram as sessões. No entanto, se configurado, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

### Grupos de entrega estáticos de SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas não atribuídas ligadas com base no número total de máquinas não atribuídas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas não atribuídas no grupo de entrega.

> **Importante:**

> Depois que todas as máquinas no grupo de entrega são atribuídas, o buffer de capacidade não desempenha um papel na ligação ou desligamento das máquinas.

> Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais não atribuídas são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

Para grupos de entrega estáticos de SO de sessão única, o Autoscale:

- Liga as máquinas atribuídas durante os horários de pico e as desliga durante os horários de menor movimento somente quando a propriedade `AutomaticPowerOnForAssigned` do grupo de entrega de SO de sessão única aplicável é definida como true.
- Liga automaticamente uma máquina durante os horários de pico se ela estiver desligada e a propriedade `AutomaticPowerOnForAssignedDuringPeak` do grupo de entrega ao qual ela pertence for definida como true.

Para entender como o buffer de capacidade funciona com máquinas atribuídas, considere o seguinte:

- O buffer de capacidade funciona somente quando o grupo de entrega tem uma ou mais máquinas não atribuídas.
- Se o grupo de entrega não tiver máquinas não atribuídas (todas as máquinas no grupo de entrega estão atribuídas), o buffer de capacidade não desempenha um papel no ligar ou desligar das máquinas.
- A propriedade `AutomaticPowerOnForAssignedDuringPeak` determina se as máquinas atribuídas são ligadas durante os horários de pico. Se for definida como true, o Autoscale mantém as máquinas ligadas durante os horários de pico. O Autoscale também as ligará mesmo que estejam desligadas.

### Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - As máquinas M1 a M3 estão atribuídas, e as máquinas M4 a M10 estão não atribuídas.

- Buffer de capacidade definido para 10% para horários de pico e fora de pico.
- De acordo com o agendamento selecionado, o Autoscale gerencia o consumo de energia das máquinas entre 09:00 e 18:00.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Início do agendamento – 09:00
  - O Autoscale liga as máquinas M1 a M3.
  - O Autoscale liga uma máquina adicional (por exemplo, M4) devido ao buffer de capacidade configurado. A máquina M4 está não atribuída.
- Um primeiro usuário faz logon
  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas não atribuídas e ligadas. Neste caso, o usuário recebe um desktop da máquina M4. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - O Autoscale começa a ligar uma máquina adicional (por exemplo, M5) para atender à demanda devido ao buffer de capacidade configurado.
- Um segundo usuário faz logon
  - O usuário recebe um desktop das máquinas ligadas não atribuídas. Neste caso, o usuário recebe um desktop da máquina M5. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - O Autoscale começa a ligar uma máquina adicional (por exemplo, M6) para atender à demanda devido ao buffer de capacidade configurado.
- Usuários fazem logoff
  - À medida que os usuários fazem logoff de seus desktops ou os desktops expiram, o Autoscale mantém as máquinas M1 a M5 ligadas entre 09:00 e 18:00. Quando esses usuários fazem logon na próxima vez, eles se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - A máquina não atribuída M6 está aguardando para servir um desktop a um usuário de entrada não atribuído.
- Fim do agendamento – 18:00
  - Às 18:00, o Autoscale desliga as máquinas M1 a M5.

- O Autoscale mantém a máquina não atribuída M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário de entrada não atribuído.
- No grupo de entrega, as máquinas M6 a M10 são máquinas não atribuídas.

## Tempos limite de sessão dinâmicos

Este recurso permite configurar tempos limite de sessão desconectada e ociosa para seus horários de pico e fora de pico de uso, a fim de obter um esvaziamento mais rápido da máquina e economia de custos. Este recurso se aplica a:

- Máquinas de SO de sessão única e multi-sessão.
- Todas as máquinas no Grupo de Entrega, independentemente de estarem marcadas para dimensionamento automático.

Um VDA relata tempos ociosos para sessões que estiveram ociosas por mais de 10 minutos, portanto, os tempos limite de sessão dinâmicos não conseguem desconectar sessões ociosas dentro de 10 minutos de inatividade. Um valor menor remove sessões persistentes mais cedo, reduzindo assim os custos.

Autoscale SO multi-sessão - tempo limite de sessão dinâmico(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/autoscale-session-timeout-ms.png)

> **Observação:**

> - Este recurso está sempre disponível para grupos de entrega de SO multi-sessão.
> - Para grupos de entrega de SO de sessão única, este recurso se aplica a VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Certifique-se de que esses VDAs tenham se registrado no Citrix Cloud™ pelo menos uma vez. Quando indisponível, a seguinte interface de usuário aparece:

> Tempo limite de sessão dinâmico indisponível(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/autoscale-session-timeout-unavailable.png)

> - Os tempos limite dinâmicos do Autoscale™ são para economia de custos. Se usados para fins de segurança, os tempos limite configurados podem entrar em conflito com

suas políticas de GPO ou do console de Gerenciamento. Quando ocorre um conflito, o tempo limite mais curto prevalece.

**Tempo limite de sessão ociosa**. Ativa ou desativa um temporizador que especifica por quanto tempo uma conexão de usuário ininterrupta é mantida se não houver entrada do usuário. Quando o temporizador expira, a sessão é colocada no estado desconectado e o **Tempo limite de sessão desconectada** se aplica. Se o **Tempo limite de sessão desconectada** estiver desativado, a sessão não é encerrada.

**Importante:**

- Se você especificar um valor menor ou igual a 10 minutos (600 segundos), o Autoscale desconecta as sessões relevantes depois que elas ficam ociosas por 10 minutos. Isso ocorre porque o Autoscale depende dos tempos ociosos de sessão que os VDAs relatam. Os VDAs relatam tempos ociosos apenas para sessões que estiveram ociosas por mais de 10 minutos.
- Uma sessão ociosa ainda pode ser colocada em um estado desconectado se o usuário interagir com ela nos últimos 5 minutos antes de atingir o tempo limite de sessão ociosa.

**Tempo limite de sessão desconectada**. Ativa ou desativa um temporizador que especifica por quanto tempo uma área de trabalho desconectada permanece bloqueada antes que a sessão seja encerrada. Se ativado, a sessão desconectada é encerrada quando o temporizador expira.

## Perguntas Frequentes

### O recurso de tempo limite de sessão dinâmico se aplica apenas a máquinas marcadas para Autoscaling?

O recurso de tempo limite de sessão dinâmico se aplica a todas as máquinas no grupo de entrega, independentemente de estarem marcadas para dimensionamento automático.

**Quando uma sessão é desconectada devido ao tempo limite de sessão dinâmica, as máquinas não marcadas também são incluídas no destino do Autoscale de máquinas marcadas?**

O recurso de tempo limite de sessão dinâmico não está relacionado ao recurso de marcação do Autoscale. Se os tempos limite de sessão dinâmicos resultarem no encerramento das sessões, as máquinas não marcadas também poderão ser desligadas durante o processo, desde que as máquinas estejam esvaziando até o desligamento.

## Dimensionamento automático de máquinas com tags (cloud burst)

> **Nota:**
>
> Este recurso era anteriormente Restrict Autoscale.

### Introdução

O Autoscale oferece a flexibilidade para gerenciar a energia de apenas um subconjunto de máquinas em um grupo de entrega. Para conseguir isso, aplique uma tag a uma ou mais máquinas e então configure o Autoscale para gerenciar a energia apenas das máquinas marcadas.

Este recurso pode ser útil em casos de uso de cloud bursting, onde você deseja usar recursos locais (ou instâncias de nuvem pública reservadas) para manipular cargas de trabalho antes que os recursos baseados em nuvem atendam à demanda adicional (ou seja, cargas de trabalho de burst). Para permitir que as máquinas locais (ou instâncias reservadas) atendam às cargas de trabalho primeiro, você deve usar a restrição de tags juntamente com a preferência de zona.

A restrição de tags especifica as máquinas a serem gerenciadas por energia pelo Autoscale. A preferência de zona especifica as máquinas na zona preferencial para manipular solicitações de inicialização do usuário. Para obter mais informações, consulte Tags e Preferência de zona.

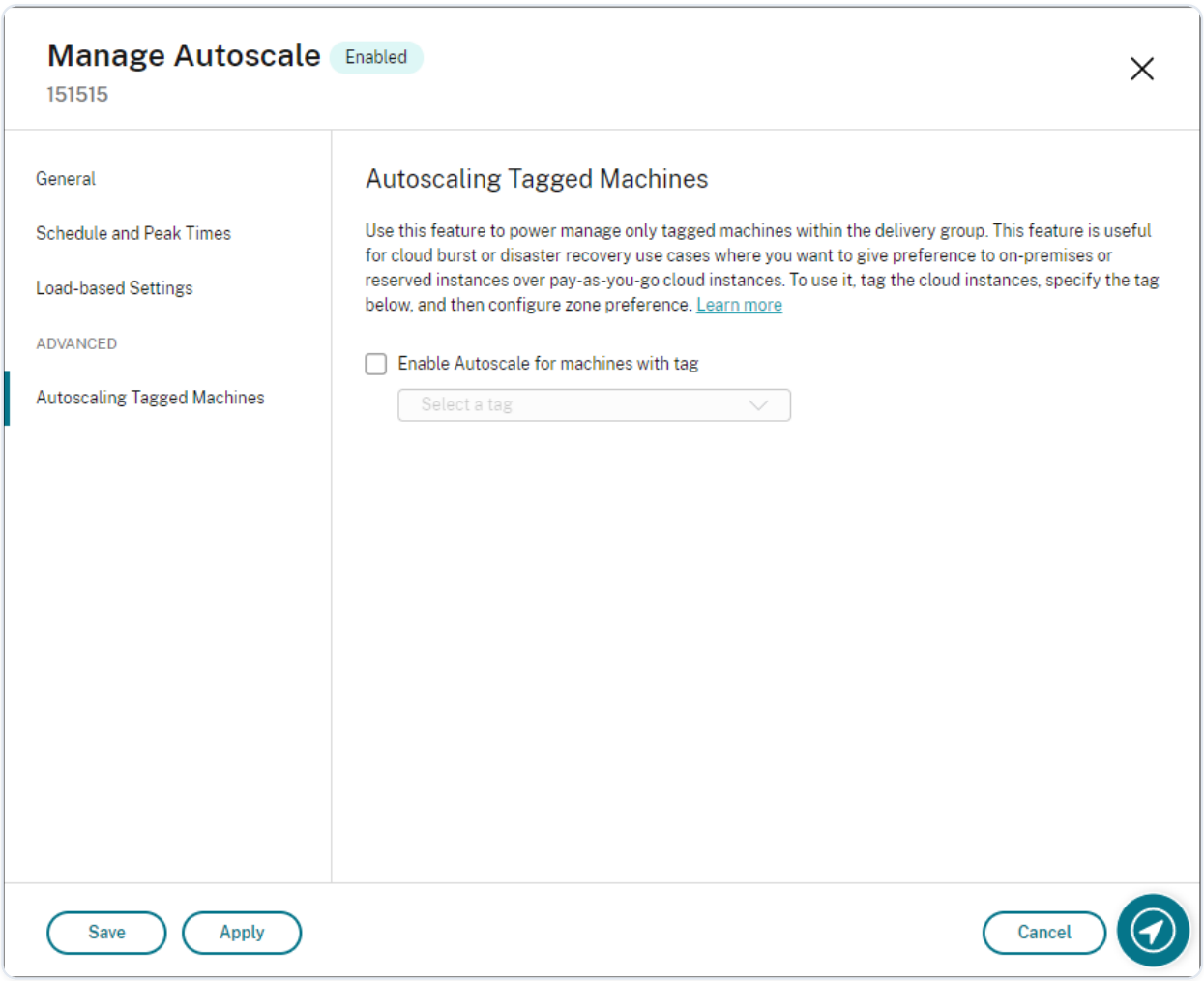
Para dimensionar automaticamente certas máquinas com tags, você pode usar o console Gerenciar ou o PowerShell.

### Use o console Gerenciar para dimensionar automaticamente certas máquinas com tags

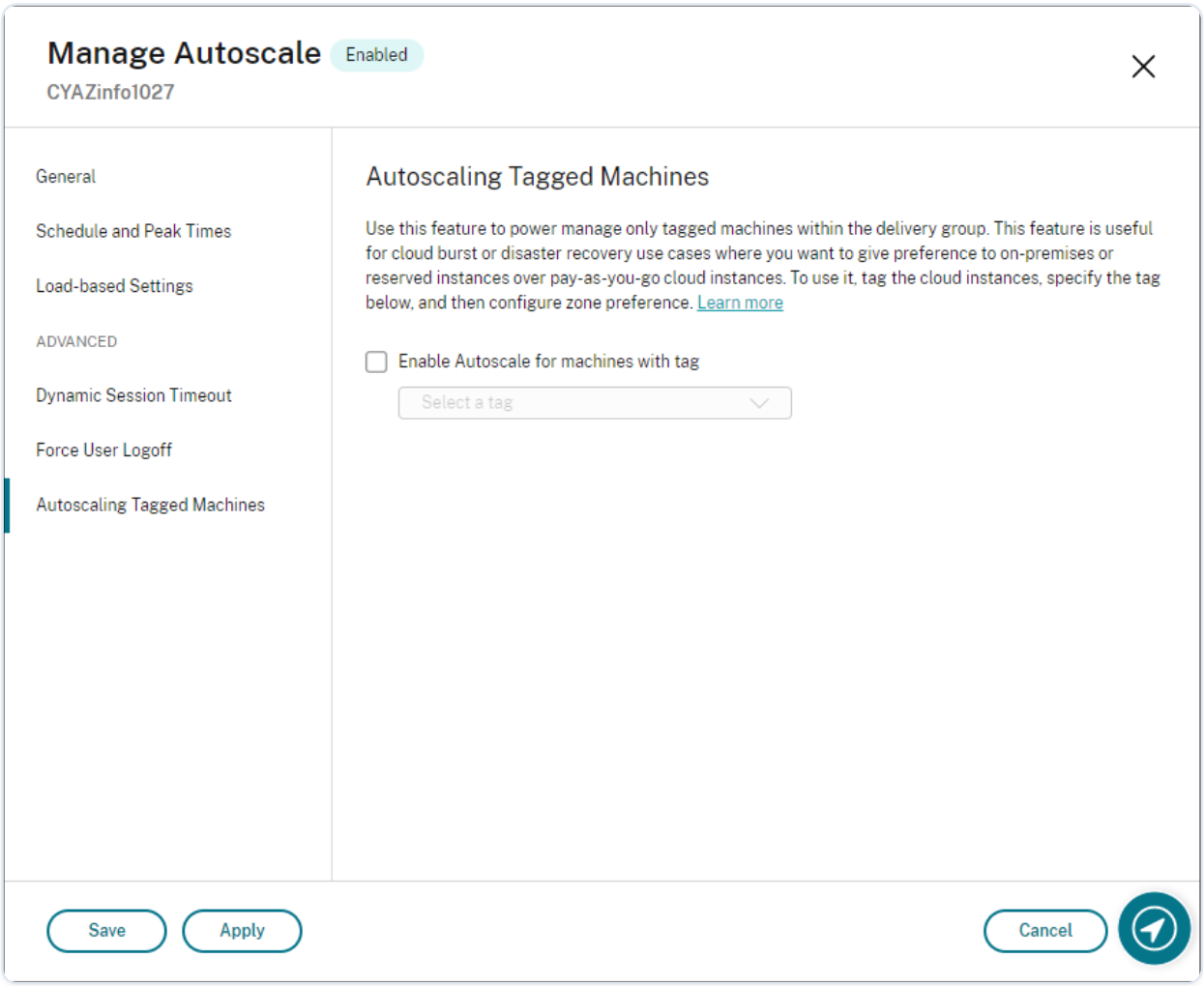
Para dimensionar automaticamente certas máquinas com tags, conclua as seguintes etapas:

1. Crie uma tag e aplique essa tag às máquinas aplicáveis no grupo de entrega. Para obter mais informações, consulte Gerenciar tags e restrições de tags.
2. Selecione o grupo de entrega e, em seguida, abra o assistente **Gerenciar Autoscale**.
3. Na página **Dimensionamento Automático de Máquinas com Tags**, selecione **Habilitar Autoscale para máquinas com tag**, selecione uma tag da lista e, em seguida, clique em **Aplicar** para salvar suas alterações.

   Interface do usuário para grupos de entrega de SO de sessão única *estáticos* e *aleatórios*:




   Interface do usuário para *grupos de entrega de SO multi-sessão*:




**Aviso:**

- O dimensionamento automático de máquinas com uma tag específica pode fazer com que o histograma seja atualizado automaticamente para refletir o número de máquinas por tag. Na página **Agendamento e Horários de Pico**, você pode atribuir máquinas manualmente a cada slot de tempo, se necessário.
- Você não pode excluir uma tag que está sendo usada em máquinas marcadas. Para excluir a tag, você deve primeiro remover a restrição da tag.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, vá para a página **Gerenciar Autoscale > Máquinas Marcadas com Autoscale** e desmarque **Habilitar Autoscale para máquinas com tag**.

**Aviso:**

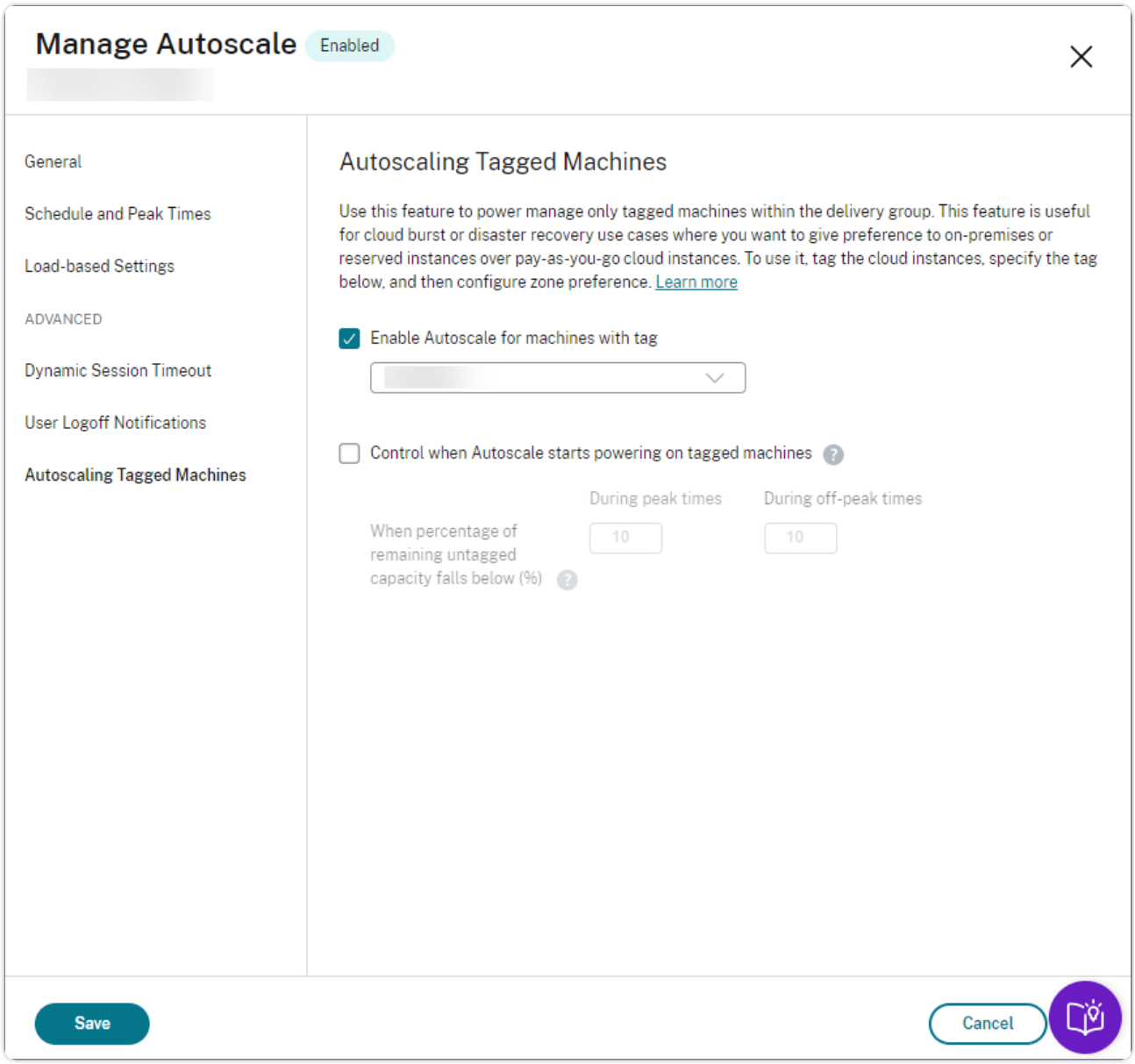
- Se você remover a tag das máquinas aplicáveis sem desmarcar **Habilitar Autoscale para máquinas com tag**, poderá receber um aviso ao abrir o assistente **Gerenciar Autoscale**. A remoção da tag das máquinas pode deixar o Autoscale sem máquinas para gerenciar, pois a tag especificada no Autoscale se tornou inválida. Para resolver o aviso, vá para a página **Máquinas Marcadas com Autoscale**, remova a tag inválida e clique em **Aplicar** para salvar suas alterações.

### Controlar quando o Autoscale liga os recursos

Você também pode controlar quando o Autoscale começa a ligar máquinas marcadas com base no uso de máquinas não marcadas. Isso ajuda a otimizar ainda mais o consumo de suas cargas de trabalho marcadas ou na nuvem pública.

Para fazer isso, conclua as seguintes etapas:

1. Na página **Máquinas Marcadas com Autoscale**, selecione **Controlar quando o Autoscale começa a ligar máquinas marcadas**.
2. Insira a porcentagem de uso de máquinas não marcadas que você deseja atingir para horários de pico e fora de pico e, em seguida, clique em **Aplicar**. Valores suportados: 0–100.




**Dica:**

A porcentagem controla quando o Autoscale começa a ligar máquinas marcadas. Quando a porcentagem cai abaixo do limite (padrão, 10%), o Autoscale começa a ligar máquinas marcadas. Quando a porcentagem excede o limite, o Autoscale entra no modo de desligamento. Ao inserir a porcentagem, considere dois cenários:

- Para grupos de entrega de SO de sessão única: O valor é definido como uma porcentagem do número total de máquinas não marcadas em estado ocioso. Exemplo: Você tem 10 máquinas de SO de sessão única não marcadas. Quando apenas uma é deixada sem uma sessão, o Autoscale começa a ligar uma máquina marcada.

- Para grupos de entrega de SO de múltiplas sessões: O valor é definido como uma porcentagem da capacidade total (em termos de índice de carga) de máquinas não marcadas disponíveis. Exemplo: Você tem 10 máquinas de SO de múltiplas sessões não marcadas. Quando elas estão 90% carregadas, o Autoscale começa a ligar uma máquina marcada.

### Usar o PowerShell para dimensionar automaticamente certas máquinas marcadas

Para usar o SDK do PowerShell diretamente, conclua as seguintes etapas:

1. **Criar uma tag.** Use o comando New-Brokertag do PowerShell para criar uma tag.
   - Por exemplo: `$managed = New-BrokerTag Managed`. Neste caso, a tag é nomeada "Managed." Para mais informações sobre o comando New-Brokertag do PowerShell, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`.
2. **Aplique a tag às máquinas**. Use o comando Get-Brokermachine do PowerShell para aplicar a tag às máquinas em um catálogo que você deseja que o Autoscale gerencie o consumo de energia.
   - Por exemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. Neste caso, o catálogo é nomeado "cloud."
   - Para mais informações sobre o comando Get-Brokermachine do PowerShell, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`.

   **Nota:**

   Você pode adicionar novas máquinas ao catálogo após aplicar a tag. A tag *NÃO* é aplicada automaticamente a essas novas máquinas.
3. **Adicione máquinas marcadas ao grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia.** Use o comando Get-BrokerDesktopGroup do PowerShell para adicionar uma restrição de tag ao grupo de entrega que contém as máquinas (em outras palavras, "restringir inicializações a máquinas com a tag X").

- Por exemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. Neste caso, o UID do Grupo de Entrega é 1.
- Para mais informações sobre o comando Get-BrokerDesktopGroup do PowerShell, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, use o comando Get-BrokerDesktopGroup do PowerShell.

Exemplo: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`. Neste caso, o UID do grupo de entrega é 1.

> **Nota:**
>
> Máquinas sem tag reiniciam automaticamente depois que os usuários as desligam. Esse comportamento garante que elas se tornem disponíveis para manipular cargas de trabalho mais cedo. Isso pode ser ativado ou desativado por grupo de desktop usando a propriedade `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

### Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do catálogo de máquinas**. Existem dois catálogos de máquinas (C1 e C2).
  - O Catálogo C1 contém 5 máquinas (M1 a M5) que são locais nas implantações no local.
  - O Catálogo C2 contém 5 máquinas (M6 a M10) que são remotas nas implantações em nuvem.
- **Restrição de tag**. Uma tag chamada "Cloud" é criada e aplicada às máquinas M6 a M10 no catálogo C2.
- **Configuração de zona**. Duas zonas (Z1 e Z2) são criadas.
  - A Zona Z1, que contém o catálogo C1, corresponde às implantações locais.
  - A Zona Z2, que contém o catálogo C2, corresponde às implantações em nuvem.

- **Configuração do grupo de entrega**
  - O grupo de entrega contém 10 máquinas (M1 a M10), 5 máquinas dos catálogos C1 (M1 a M5) e 5 do catálogo C2 (M6 a M10).
  - As máquinas M1 a M5 são ligadas manualmente e permanecem ligadas durante todo o agendamento.
- **Configuração do Autoscale**
  - O buffer de capacidade é definido como 10%.
  - O Autoscale gerencia apenas máquinas com a tag "Cloud". Neste caso, o Autoscale gerencia as máquinas em nuvem M6 a M10.
- **Configuração de aplicativo ou desktop publicado**. As preferências de zona são configuradas para os desktops publicados (por exemplo), onde a Zona Z1 é preferida em relação à Zona Z2 para uma solicitação de inicialização do usuário.
  - A Zona Z1 é configurada como a zona preferencial (zona inicial) para os desktops publicados.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. Sessões de usuário aumentam.
3. As sessões de usuário aumentam ainda mais até que todas as máquinas locais disponíveis sejam consumidas.
4. Mais sessões de usuário são iniciadas.
5. A sessão de usuário diminui devido ao encerramento da sessão.
6. A sessão de usuário diminui ainda mais até que a carga da sessão seja tratada apenas por máquinas locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - As máquinas locais M1 a M5 estão todas ligadas.
  - Uma máquina na nuvem (por exemplo, M6) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina é ligada.

    - O valor do índice de carga de todas as máquinas ligadas (M1 a M6) está em uma carga de linha de base (índice de carga igual a 0).

- Usuários fazem logon
    - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas entre essas máquinas locais.
    - O valor do índice de carga das máquinas ligadas (M1 a M5) aumenta.
    - O valor do índice de carga da máquina ligada M6 está em uma carga de linha de base.
- Usuários aumentam a carga, consumindo todos os recursos locais
    - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas entre essas máquinas locais.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 permanece em uma carga de linha de base.
- Mais um usuário faz login
    - A sessão excede a preferência de zona e é direcionada para ser hospedada na máquina em nuvem M6.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 aumenta e não está mais em uma carga de linha de base. Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M7) para atender à demanda devido ao buffer de capacidade configurado. Observe que pode levar algum tempo para ligar a máquina M7. Portanto, pode haver um atraso até que a máquina M7 esteja pronta.
- Mais usuários fazem login
    - As sessões são direcionadas para serem hospedadas na máquina M6.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 aumenta ainda mais, mas a capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
    - O valor do índice de carga da máquina ligada M7 permanece em uma carga de linha de base.

- Ainda mais usuários fazem login
  - Depois que a máquina M7 estiver pronta, as sessões são direcionadas para serem hospedadas nas máquinas M6 e M7 e são balanceadas entre essas máquinas.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina M7 não está mais em uma carga de linha de base.
  - O valor do índice de carga das máquinas ligadas (M6 e M7) aumenta.
  - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
- A carga da sessão do usuário diminui devido ao encerramento da sessão
  - Depois que os usuários saem de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M7 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas em nuvem (M6 a M7) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina (por exemplo, M7), a menos que novas alterações ocorram; por exemplo, a carga do usuário aumenta novamente ou outras máquinas em nuvem se tornam menos carregadas.
- A carga da sessão do usuário diminui ainda mais até que uma ou mais máquinas em nuvem não sejam mais necessárias
  - Depois que todas as sessões na máquina M7 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M7.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) pode cair para um nível abaixo de 10.000.
  - O valor do índice de carga da máquina ligada (M6) diminui.
- A sessão do usuário diminui ainda mais até que nenhuma máquina em nuvem seja necessária.
  - Mesmo que não haja sessões de usuário na máquina M6, o Autoscale não a desliga porque ela está reservada como capacidade sobressalente.
  - O Autoscale mantém a máquina em nuvem restante M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário que está chegando.

- As sessões não são direcionadas para serem hospedadas na máquina M6 enquanto as máquinas locais tiverem capacidade disponível.

## Notificações de logoff do usuário (anteriormente forçar logoff do usuário)

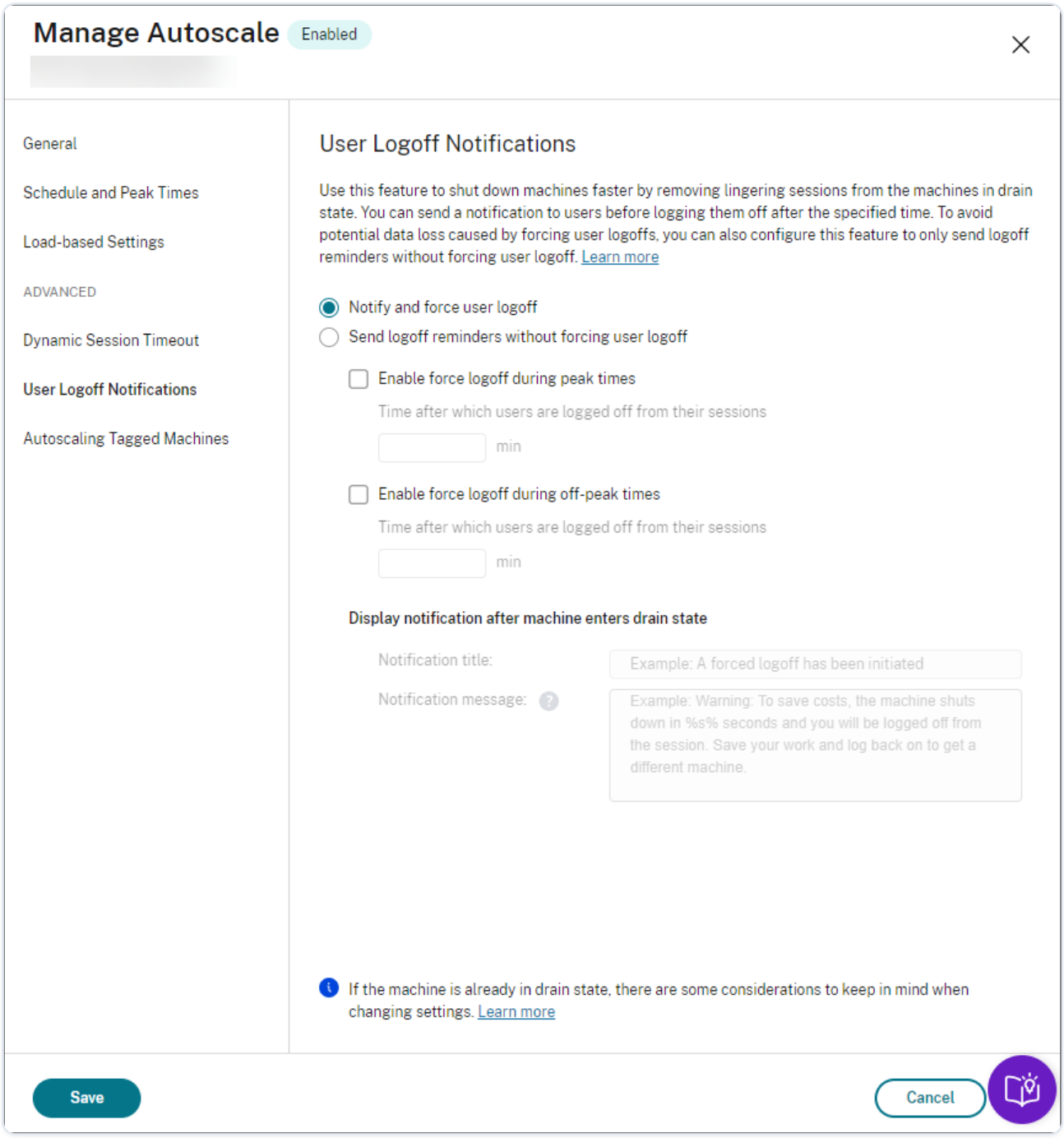
> **Importante:**
>
> Este recurso está disponível apenas na interface do usuário do Autoscale™ para grupos de entrega baseados em aplicativos de várias sessões.
>
> Para melhor alcançar a economia de custos, o Autoscale permite que você force o logoff de sessões persistentes. Ele faz isso permitindo que você envie uma notificação personalizada aos usuários e especifique um período de carência após o qual as sessões são forçadas a fazer logoff. Isso é feito apenas para máquinas em estado de drenagem e não para todas as máquinas ligadas. Para evitar a potencial perda de dados causada pelo logoff forçado de usuários, você pode configurar este recurso para apenas enviar lembretes de logoff sem forçar o logoff do usuário.

Você tem as duas opções a seguir:

- **Notificar e forçar o logoff do usuário**
- **Enviar lembretes de logoff sem forçar o logoff do usuário**

### Notificar e forçar o logoff do usuário

Se selecionado, o Autoscale desconecta os usuários de suas sessões após os horários especificados abaixo.




**Habilitar logoff forçado durante horários de pico**. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de pico quando o tempo especificado expira.

**Habilitar logoff forçado durante horários de menor movimento**. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de menor movimento quando o tempo especificado expira.

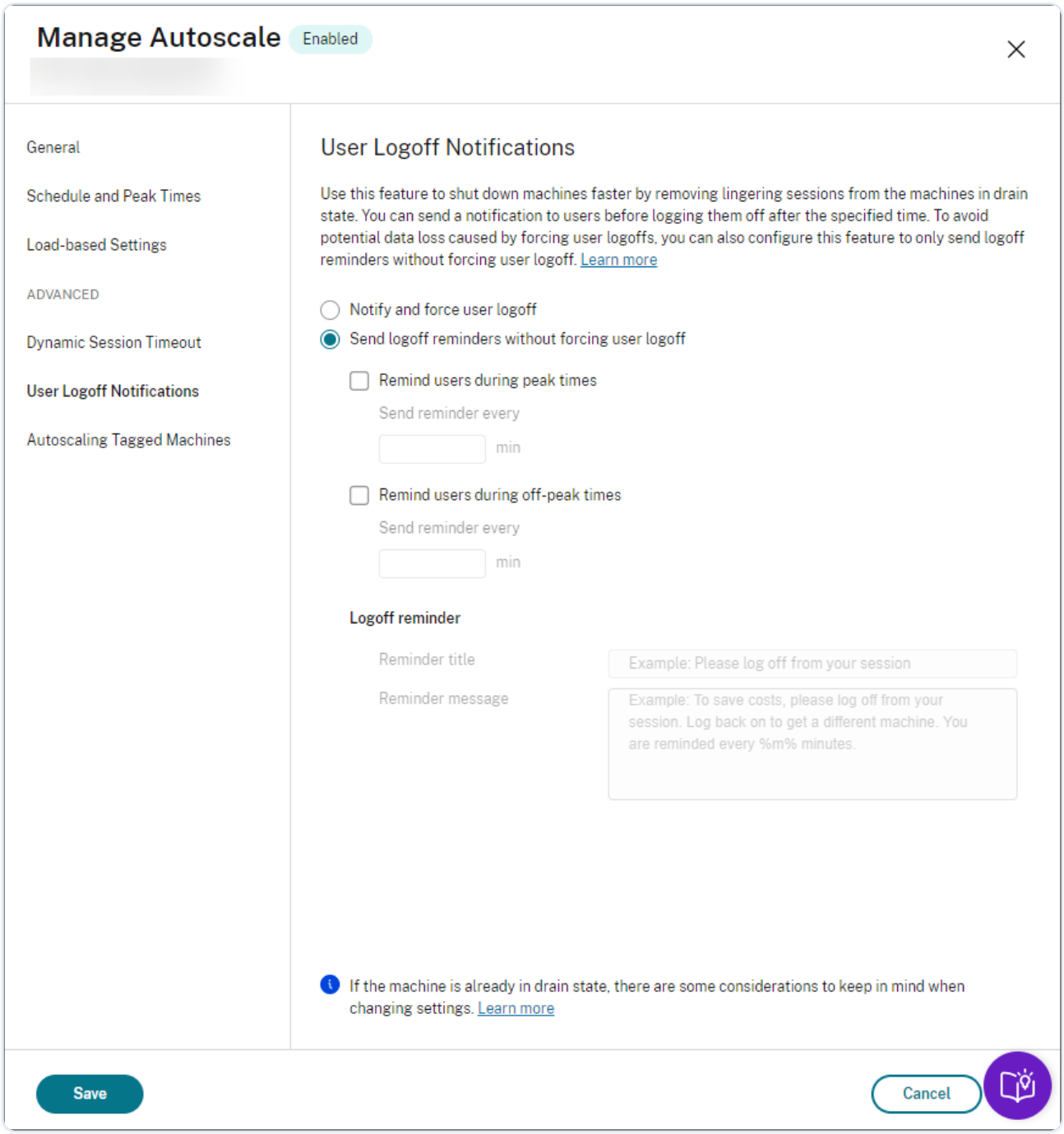
**Exibir notificação depois que a máquina entrar no estado de drenagem**. Permite que você envie notificações aos usuários depois que a máquina deles entrar no estado de drenagem.

- **Título da notificação**. Permite que você especifique um título para a notificação a ser enviada aos usuários. Exemplo: `A forced logoff has been initiated.`.

- **Mensagem de notificação**. Permite especificar o conteúdo da notificação a ser enviada aos usuários. Você pode usar %s% ou %m% como variáveis para indicar o tempo especificado na mensagem. Para expressar o tempo em segundos, use %s%. Para expressar o tempo em minutos, use %m%. Exemplo: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

### Enviar lembretes de logoff sem forçar o logoff do usuário

Se selecionado, os usuários receberão um lembrete para fazer logoff de sua máquina depois que ela entrar no estado de drenagem. Este lembrete pode ser configurado para ser enviado no intervalo especificado abaixo.




**Lembrar usuários durante horários de pico**. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de pico a cada X minutos (X denota o tempo especificado).

**Lembrar usuários durante horários de menor movimento**. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de menor movimento a cada X minutos (X denota o tempo especificado).

**Lembrete de logoff**. Permite configurar o lembrete enviado aos usuários depois que a máquina entra no estado de drenagem.

- **Título do lembrete**. Permite especificar um título para o lembrete a ser enviado aos usuários. Exemplo: `Please log off from your session`.
- **Mensagem do lembrete**. Permite especificar uma mensagem a ser enviada aos usuários. Exemplo: `Please log off from your session and log back on to save costs`.

### Considerações

Se a máquina já estiver em estado de drenagem, considere o seguinte ao alterar as configurações:

- Se você alterar a configuração de **Enviar lembretes de logoff sem forçar o logoff do usuário** para **Notificar e forçar o logoff do usuário**, a nova configuração entra em vigor imediatamente.
- Se você alterar a configuração de **Notificar e forçar o logoff do usuário** para **Enviar lembretes de logoff sem forçar o logoff do usuário**, a nova configuração não entrará em vigor até a próxima vez que a máquina entrar no estado de drenagem. O usuário ainda é forçado a fazer logoff.

## Comandos do SDK do PowerShell do Broker

Você pode configurar o Autoscale para grupos de entrega usando o SDK do Broker PowerShell. Para configurar o Autoscale usando comandos do PowerShell, você deve usar a versão 7.21.0.12 ou posterior do SDK do PowerShell. Para obter mais informações sobre os SDKs do PowerShell, consulte SDKs e APIs.

### Set-BrokerDesktopGroup

Desabilita ou habilita um BrokerDesktopGroup existente ou altera suas configurações. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

#### Exemplos

Consulte os exemplos a seguir para obter detalhes sobre como usar os cmdlets do PowerShell.

Habilitar Autoscale™

- Suponha que você queira habilitar o Autoscale para o grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

Configure o buffer de capacidade separadamente para horários de pico e fora de pico

- Suponha que você queira definir o buffer de capacidade para 20% para horários de pico e 10% para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

Configurar a configuração de **tempo limite de desconexão**

- Suponha que você queira definir o valor de **tempo limite de desconexão** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

Configurar a configuração de **tempo limite de logoff**

- Suponha que você queira definir o valor de **tempo limite de logoff** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Configurar a configuração de **atraso de desligamento**

- Suponha que você queira definir o atraso de desligamento para 15 minutos para um grupo de entrega cujo nome é "MyDesktop." Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

Configurar um período de tempo durante o qual o atraso de desligamento não entra em vigor

- Suponha que você queira que o atraso de desligamento entre em vigor até que 30 minutos tenham decorrido para um grupo de entrega cujo nome é "MyDesktop." Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`.

Configurar a definição de **custo da instância da máquina**

- Suponha que você queira definir o custo da instância da máquina por hora para 0,2 dólares para um grupo de entrega cujo nome é "MyDesktop." Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

### New-BrokerPowerTimeScheme

Cria um BrokerPowerTimeScheme para um grupo de entrega. Para mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`.

#### Exemplo

Suponha que você queira criar um esquema de tempo de energia para um grupo de entrega cujo valor UID é 3. O novo esquema abrange o fim de semana, segunda e terça-feira. O período das 8:00 AM às 6:30 PM é definido como horários de pico para os dias incluídos no esquema. Para horários de pico, o tamanho do pool (o número de máquinas mantidas ligadas) é 20. Para horários fora de pico, é 5. Você pode usar o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

### Parâmetros para tempos limite de sessão dinâmicos

Os seguintes cmdlets do SDK do Broker PowerShell foram estendidos para tempos limite de sessão dinâmicos, suportando vários novos parâmetros:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Esses parâmetros incluem:

- **DisconnectPeakIdleSessionAfterSeconds** – Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante o horário de pico. Esta propriedade tem um valor

padrão de 0, o que indica a desativação do seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento para o grupo de entrega apenas durante o horário de pico.

- **DisconnectOffPeakIdleSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante o horário fora de pico. O valor padrão desta propriedade é 0, o que indica a desativação do seu comportamento associado durante o horário fora de pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário fora de pico.
- **LogoffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de pico.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de não pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de não pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega somente durante o horário de não pico.

### Exemplo

Suponha que você queira definir o tempo limite de sessão ociosa para 3.600 segundos durante os horários de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

Isso desconecta as sessões que ficaram ociosas por mais de 1 hora fora do pico para o grupo de desktops cujo nome é "MyDesktop".

# Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios. Seus recursos de instrumentação e telemetria permitem que usuários técnicos (clientes, parceiros e engenheiros) autodiagnostiquem e corrijam problemas e otimizem seus ambientes. Para obter detalhes e as informações mais recentes sobre o CIS e como ele funciona, consulte `<https://cis.citrix.com>` (credenciais de conta Citrix necessárias).

Todas as informações carregadas para a Citrix são usadas para fins de solução de problemas e diagnóstico, e para melhorar a qualidade, confiabilidade e desempenho dos produtos, sujeitas a:

- Política do Citrix Insight Services em `<https://cis.citrix.com/legal>`
- Política de Privacidade da Citrix em `<https://www.cloud.com/privacy-policy>`

Esta versão do Citrix Virtual Apps and Desktops™ oferece suporte às seguintes tecnologias.

- Análise de instalação e atualização do Citrix Virtual Apps and Desktops
- Programa de Melhoria da Experiência do Cliente Citrix (CEIP)
- Citrix Call Home
- Citrix Scout

Além (e separadamente) do CIS e do Citrix Analytics: o Google Analytics é coletado (e posteriormente carregado) automaticamente quando você instala (ou atualiza) o Studio. Após instalar o Studio, você pode alterar essa configuração com a chave de registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Um valor de 1 habilita a coleta e o upload, 0 desabilita a coleta e o upload.

## Análise de instalação e atualização

Ao usar o instalador completo do produto para implantar ou atualizar componentes do Citrix Virtual Apps and Desktops, informações anônimas sobre o processo de instalação são coletadas e armazenadas na máquina onde você está instalando/atualizando o componente. Esses dados são usados para ajudar a Citrix a melhorar as experiências de instalação de seus clientes.

As informações são armazenadas localmente em `%ProgramData%\Citrix\CTQs`.

O upload automático desses dados é habilitado por padrão nas interfaces gráfica e de linha de comando do instalador completo do produto.

- Você pode alterar o valor padrão em uma configuração de registro. Se você alterar a configuração de registro antes de instalar/atualizar, esse valor será usado quando você usar o instalador completo do produto.
- Você pode substituir a configuração padrão se instalar/atualizar com a interface de linha de comando especificando uma opção com o comando.

**Controlar uploads automáticos:**

- Configuração de registro que controla o upload automático de análises de instalação/atualização (padrão = 1):

  - Local: `HKLM:\Software\Citrix\MetaInstall`
  - Nome: SendExperienceMetrics
  - Valor: 0 = desativado, 1 = ativado

- Usando o PowerShell, o seguinte cmdlet desativa o upload automático de análises de instalação/atualização:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- Para desativar uploads automáticos com o comando XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, inclua a opção `/disableexperiencemetrics`.

  Para ativar uploads automáticos com o comando XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, inclua a opção `/sendexperiencemetrics`.

## Programa de Melhoria da Experiência do Cliente Citrix

Ao participar do Programa de Melhoria da Experiência do Cliente Citrix (CEIP), estatísticas anônimas e informações de uso são enviadas à Citrix para ajudar a Citrix a melhorar a qualidade e o desempenho dos produtos Citrix. Para obter mais informações, consulte https://more.citrix.com/XD-CEIP.

### Inscrição durante a criação ou atualização do Site

Você é automaticamente inscrito no CEIP ao criar um Site (depois de instalar o primeiro Delivery Controller™). O primeiro upload de dados ocorre aproximadamente sete dias após a criação do Site.

Você pode interromper sua participação a qualquer momento após a criação do Site. Selecione o nó **Configurações** no painel esquerdo do Web Studio e desative a configuração **Programa de Melhoria da Experiência do Cliente Citrix**.

Ao atualizar uma implantação do Citrix Virtual Apps and Desktops:

- Se você atualizar de uma versão que não suportava o CEIP, será perguntado se deseja participar.
- Se você atualizar de uma versão que suportava o CEIP e a participação estava ativada, o CEIP será ativado no Site atualizado.

- Se você atualizar de uma versão que suportava o CEIP e a participação estava desativada, o CEIP será desativado no Site atualizado.
- Se você atualizar de uma versão que suportava o CEIP e a participação é desconhecida, será perguntado se deseja participar.

As informações coletadas são anônimas, portanto, não podem ser visualizadas depois de serem carregadas para o Citrix Insight Services.

### Inscrição ao instalar um VDA

Por padrão, você é automaticamente inscrito no CEIP ao instalar um VDA do Windows. Você pode alterar esse padrão em uma configuração de registro. Se você alterar a configuração de registro antes de instalar o VDA, esse valor será usado.

Configuração de registro que controla a inscrição automática no CEIP (padrão = 1):

Local: `HKLM:\Software\Citrix\Telemetry\CEIP` Nome: Enabled Valor: 0 = desativado, 1 = ativado

Por padrão, a propriedade `Enabled` está oculta no registro. Quando não especificada, o recurso de upload automático é ativado.

Usando o PowerShell, o seguinte cmdlet desativa a inscrição no CEIP:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

Os pontos de dados de tempo de execução coletados são periodicamente gravados como arquivos em uma pasta de saída (padrão %programdata%/Citrix/VdaCeip).

O primeiro upload de dados ocorre aproximadamente sete dias após a instalação do VDA.

### Inscrição ao instalar outros produtos e componentes

Você também pode participar do CEIP ao instalar produtos, componentes e tecnologias Citrix relacionados, como Citrix Provisioning™, AppDNA, Citrix License Server, aplicativo Citrix Workspace™ para Windows, Universal Print Server e Session Recording. Consulte a documentação deles para obter detalhes sobre a instalação e os valores padrão de participação.

# Citrix Call Home

Ao instalar certos componentes e recursos no Citrix Virtual Apps and Desktops, você tem a oportunidade de participar do Citrix Call Home. O Call Home coleta dados de diagnóstico e então periodicamente carrega pacotes de telemetria contendo esses dados diretamente para o Citrix Insight Services (via HTTPS na porta padrão 443) para análise e solução de problemas.

No Citrix Virtual Apps and Desktops, o Call Home é executado como um serviço em segundo plano sob o nome Citrix Telemetry Service. Para obter mais informações, consulte https://more.citrix.com/XD-CALLHOME.

A funcionalidade de agendamento do Call Home também está disponível no Citrix Scout. Para obter detalhes, consulte Citrix Scout.

## O que é coletado

O rastreamento do Citrix Diagnostic Facility (CDF) registra informações que podem ser úteis para a solução de problemas. O Call Home coleta um subconjunto de rastreamentos CDF que podem ser úteis ao solucionar falhas comuns, por exemplo, registros de VDA e inicializações de aplicativos/desktops. Essa tecnologia é conhecida como rastreamento sempre ativo (AOT). Os logs AOT são salvos em disco em C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT.

O Call Home não coleta nenhuma outra informação de Event Tracing for Windows (ETW), nem pode ser configurado para fazê-lo.

O Call Home também coleta outras informações, como:

- Registros criados pelo Citrix Virtual Apps and Desktops em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informações do Windows Management Instrumentation (WMI) no namespace Citrix.
- Lista de processos em execução.
- Dumps de falha de processos Citrix que são armazenados em `%PROGRAMDATA%\Citrix\CDF`.
- Informações de instalação e atualização. Isso pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront™, logs de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

As informações de rastreamento são compactadas à medida que são coletadas. O Citrix Telemetry Service retém um máximo de 10 MB de informações de rastreamento recentes compactadas, com um limite de tempo máximo de oito dias.

- A compactação de dados permite que o Call Home mantenha uma pequena pegada no VDA.
- Os rastreamentos são mantidos em memória para evitar IOPs em máquinas provisionadas.
- O buffer de rastreamento usa um mecanismo circular para reter rastreamentos na memória.

O Call Home coleta os principais pontos de dados listados em Pontos de dados chave do Call Home.

### Resumo de configuração e gerenciamento

Você pode se inscrever no Call Home ao usar o assistente de instalação do produto completo ou posteriormente, usando cmdlets do PowerShell. Ao se inscrever, por padrão, os diagnósticos são coletados e enviados para a Citrix todo domingo, aproximadamente às 3:00 AM, horário local. O upload é randomizado com um intervalo de duas horas a partir do horário especificado. Isso significa que um upload usando o agendamento padrão ocorre entre 3:00 AM e 5:00 AM.

Se você não quiser carregar informações de diagnóstico de forma agendada (ou se quiser alterar um agendamento), você pode usar cmdlets do PowerShell para coletar e carregar diagnósticos manualmente ou armazená-los localmente.

Ao se inscrever em uploads agendados do Call Home e ao carregar manualmente informações de diagnóstico para a Citrix, você fornece credenciais de conta Citrix ou Citrix Cloud™. A Citrix troca as credenciais por um token de upload que é usado para identificar o cliente e carregar os dados. As credenciais não são salvas.

Quando um upload ocorre, uma notificação é enviada por e-mail para o endereço associado à conta Citrix.

Se você habilitar o Call Home ao instalar um componente, você pode desativá-lo mais tarde.

### Pré-requisitos

- A máquina deve estar executando o PowerShell 3.0 ou posterior.
- O Serviço de Telemetria Citrix deve estar em execução na máquina.
- A variável de sistema `PSModulePath` deve ser definida para o caminho de instalação da Telemetria, por exemplo, `C:\Program Files\Citrix\Telemetry Service\`.

### Ativar o Call Home durante a instalação do componente

**Durante a instalação ou atualização do VDA:** Ao instalar ou atualizar um Virtual Delivery Agent usando a interface gráfica no instalador completo do produto, você será perguntado se deseja participar do Call Home. Existem duas opções:

- Participar do Call Home.
- Não participar do Call Home.

Se você estiver atualizando um VDA e já tiver se inscrito no Call Home, essa página do assistente não aparecerá.

**Durante a instalação ou atualização do Controller:** Ao instalar ou atualizar um Delivery Controller usando a interface gráfica, você será perguntado se deseja participar do Call Home. Existem três opções:

Ao instalar um Controller, você não pode configurar informações na página Call Home do assistente de instalação se esse servidor tiver um GPO do Active Directory com a configuração de política "Fazer logon como um serviço" aplicada. Para obter detalhes, consulte CTX218094.

Se você estiver atualizando um Controller e já tiver se inscrito no Call Home, não será perguntado sobre a participação.

### Cmdlets do PowerShell

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nestes casos de uso comuns.

Para usar um servidor proxy para uploads, consulte Configurar um servidor proxy.

- **Habilitar uploads agendados:** As coletas de diagnóstico são automaticamente carregadas para a Citrix. Se você não inserir cmdlets adicionais para um agendamento personalizado, o agendamento padrão será usado.

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  Para confirmar se os uploads agendados estão habilitados, digite `Get-CitrixCallHome`. Se habilitado, o retorno é `IsEnabled=True` e `IsMasterImage=False`.

- **Habilitar uploads agendados para máquinas criadas a partir de uma imagem mestre:** Habilitar uploads agendados em uma imagem mestre elimina a necessidade de configurar cada máquina criada no catálogo de máquinas.

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

Para confirmar se os uploads agendados estão habilitados, digite **Get-CitrixCallHome**. Se habilitado, o retorno é `IsEnabled=True` e `IsMasterImage=True`.

- **Criar um agendamento personalizado:** Crie um agendamento diário ou semanal para coletas e uploads de diagnóstico.

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

**Exemplos:**

O cmdlet a seguir cria um agendamento para agrupar e carregar dados às 10:20 todas as noites. O parâmetro Hours usa um relógio de 24 horas. Quando o valor do parâmetro `UploadFrequency` é Daily, o parâmetro `DayOfWeek` é ignorado, se especificado.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Para confirmar o agendamento, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, ele retorna `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`.

O cmdlet a seguir cria um agendamento para agrupar e carregar dados às 10:20 de toda quarta-feira à noite.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

Para confirmar o agendamento, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, ele retorna `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`.

### Desabilitar Call Home

Você pode desabilitar o Call Home usando um cmdlet do PowerShell ou através do Citrix Scout.

Os logs AOT são coletados e salvos em disco, mesmo quando os uploads agendados do Call Home estão desabilitados. (Quando os uploads agendados estão desabilitados, os logs AOT não

são carregados automaticamente para a Citrix.) Você pode desabilitar a coleta e o armazenamento local dos logs AOT.

#### Desabilitar Call Home com PowerShell

Após executar o cmdlet a seguir, os dados de diagnóstico não serão carregados para a Citrix automaticamente. (Você ainda pode carregar dados de diagnóstico usando o Citrix Scout ou cmdlets do PowerShell de telemetria.)

```
Disable-CitrixCallHome
```

Para confirmar que o Call Home está desabilitado, digite `Get-CitrixCallHome`. Se desabilitado, o retorno é `IsEnabled=False` e `IsMasterImage=False`.

#### Desabilitar um agendamento de coleta usando o Citrix Scout

Para desabilitar um agendamento de coleta de diagnóstico usando o Citrix Scout, siga as orientações em Agendar coletas. Na etapa 3, clique em **Desativar** para cancelar o agendamento para as máquinas selecionadas.

#### Desabilitar a coleta de logs AOT

Após executar o seguinte cmdlet (com o campo `Enabled` definido como `false`), os logs AOT não serão coletados.

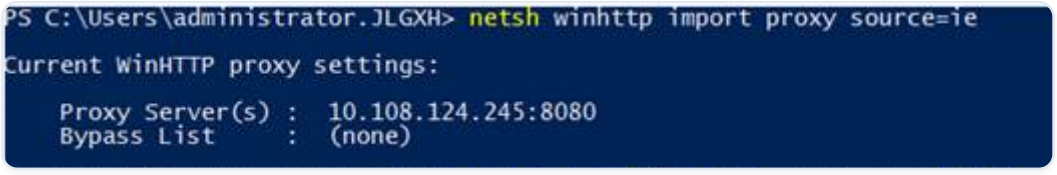
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

O parâmetro `Listen` contém argumentos no formato JSON.

### Configurar um servidor proxy para uploads do Call Home

Conclua as seguintes tarefas na máquina onde o Call Home está ativado. Os diagramas de exemplo no procedimento a seguir contêm o endereço do servidor e a porta 10.158.139.37:3128. Suas informações serão diferentes.

1. Adicione as informações do servidor proxy em seu navegador. No Internet Explorer, selecione **Opções da Internet \> Conexões \> Configurações da LAN**. Selecione **Usar um servidor proxy para sua LAN** e insira o endereço do servidor proxy e o número da porta.
2. No PowerShell, execute `netsh winhttp import proxy source=ie`.



3. Usando um editor de texto, edite o arquivo de configuração TelemetryService.exe, que está localizado em `C:\Program Files\Citrix\Telemetry Service`. Adicione as informações mostradas na caixa vermelha.




4. Reinicie o Serviço de Telemetria.

Execute os cmdlets do Call Home no PowerShell.

### Coletar e carregar informações de diagnóstico manualmente

Você pode usar o site do CIS para carregar um pacote de informações de diagnóstico para o CIS. Você também pode usar cmdlets do PowerShell para coletar e carregar informações de diagnóstico para o CIS.

Para carregar um pacote usando o site do CIS:

1. Faça logon no Citrix Insight Services usando suas credenciais de conta Citrix.
2. Selecione **Meu Espaço de Trabalho**.
3. Selecione **Healthcheck** e, em seguida, navegar até o local dos seus dados.

O CIS oferece suporte a vários cmdlets do PowerShell que gerenciam uploads de dados. Esta documentação abrange os cmdlets para dois casos comuns:

- Use o `Start-CitrixCallHomeUpload` cmdlet para coletar e carregar manualmente um pacote de informações de diagnóstico para o CIS. (O pacote não é salvo localmente.)
- Use o `Start-CitrixCallHomeUpload` cmdlet para coletar dados manualmente e armazenar um pacote de informações de diagnóstico localmente. Isso permite que você visualize os dados. Mais tarde, use o `Send-CitrixCallHomeBundle` cmdlet para carregar manualmente

uma cópia desse pacote para o CIS. (Os dados que você salvou originalmente permanecem localmente.)

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Ao inserir um cmdlet para carregar dados para o CIS, você será solicitado a confirmar o upload. Se o cmdlet expirar antes que o upload seja concluído, verifique o status do upload no log de eventos do sistema. A solicitação de upload pode ser rejeitada se o serviço já estiver realizando um upload.

**Coletar dados e carregar pacote para o CIS:**

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

**Coletar dados e salvá-los localmente:**

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

Os seguintes parâmetros são válidos:

- **Credential:** Direciona o upload para o CIS.
- **InputPath:** Local do arquivo zip a ser incluído no pacote. Este pode ser um arquivo adicional que o Suporte Citrix solicita. Certifique-se de incluir a extensão .zip.
- **OutputPath:** Local onde as informações de diagnóstico são salvas. Este parâmetro é obrigatório ao salvar dados do Call Home localmente.
- **Description and Incident Time:** Informações de formato livre sobre o upload.
- **SRNumber:** Número de incidente do Suporte Técnico Citrix.
- **Name:** Nome que identifica o pacote.
- **UploadHeader:** String formatada em JSON especificando os cabeçalhos de upload carregados para o CIS.

- **AppendHeaders:** String formatada em JSON especificando os cabeçalhos anexados carregados para o CIS.
- **Coletar:** String formatada em JSON especificando quais dados coletar ou omitir, no formato {'collector':{'enabled':Boolean}}, onde Boolean é true ou false. Os valores válidos para o coletor são:
  - 'Instrumentação de Gerenciamento do Windows'
  - 'processo'
  - 'registro'
  - 'relatório de falha'
  - 'rastreamento'
  - 'arquivo'
  - 'Pacote do Windows Installer'
  - 'dados locais'
  - 'dados do site'
  - 'Skype para Empresas'

  Por padrão, todos os coletores, exceto 'sfb', estão habilitados.

  O coletor 'sfb' foi projetado para ser usado sob demanda para diagnosticar problemas do Skype for Business. Além do parâmetro 'enabled', o coletor 'sfb' suporta os parâmetros 'account' e 'accounts' para especificar usuários de destino. Use um dos formatos:

  - "-Collect "`{'sfb':{'account':'domain\user1'}}`"
  - "-Collect "`{'sfb':{'accounts':['domain\user1', 'domain\user2']}}`"
- **Parâmetros Comuns:** Consulte a ajuda do PowerShell.

**Carregar dados que foram salvos localmente anteriormente:**

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string
[<CommonParameters>]
```

O parâmetro `Path` especifica o local do pacote salvo anteriormente.

**Exemplos:**

O cmdlet a seguir solicita o upload de dados do Call Home (excluindo dados do coletor WMI) para o CIS. Esses dados se referem a falhas de registro de VDAs do Citrix Provisioning, que foram observadas às 14h30 para o caso de Suporte Citrix 123456. Além dos dados do Call Home, o arquivo "`c:\Diagnostics\ExtraData.zip`" é incorporado ao pacote carregado.

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

O cmdlet a seguir salva dados do Call Home relacionados ao caso de Suporte Citrix 223344, observado às 8h15. Os dados são salvos no arquivo mydata.zip em um compartilhamento de rede. Além dos dados do Call Home, o arquivo "`c:\Diagnostics\ExtraData.zip`" será incorporado ao pacote salvo.

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

O cmdlet a seguir carrega o pacote de dados que você salvou anteriormente.

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

# Citrix Scout

## Introdução

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manter sua implantação do Citrix Virtual Apps and Desktops™. A Citrix oferece análise abrangente e automatizada de coleções de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

Você pode carregar arquivos de coleta para a Citrix para análise e orientação do Suporte Citrix. Ou, você pode salvar uma coleta localmente para sua própria revisão e, em seguida, carregar o arquivo de coleta para a Citrix para análise.

O Scout oferece os seguintes procedimentos:

- **Coletar:** Executa uma coleta de diagnóstico única nas máquinas que você seleciona em um site. Você pode então carregar o arquivo para a Citrix ou salvá-lo localmente.
- **Rastrear e Reproduzir:** Inicia um rastreamento manual nas máquinas que você seleciona. Em seguida, você recria problemas nessas máquinas. Após recriar o problema, o rastreamento é interrompido. O Scout então coleta outros diagnósticos e carrega o arquivo para a Citrix, ou salva o arquivo localmente.
- **Agendar:** Agenda coletas de diagnóstico para ocorrerem diariamente ou semanalmente em um horário especificado nas máquinas que você seleciona. O arquivo é automaticamente carregado para a Citrix.
- **Verificação de Integridade:** Executa verificações que avaliam a integridade e a disponibilidade do site e seus componentes. Você pode executar verificações de integridade para Delivery Controllers, Virtual Delivery Agents (VDAs), servidores StoreFront™ e Citrix License Servers. Se problemas forem encontrados durante as verificações, o Scout fornece um relatório detalhado. Cada vez que o Scout inicia, ele verifica se há scripts de verificação de integridade atualizados. Se novas versões estiverem disponíveis, o Scout as baixa automaticamente, para uso na próxima vez que as verificações de integridade forem executadas.

> **Observação:**
>
> Os procedimentos **Rastrear e Reproduzir**, **Agendar** e **Verificação de Integridade** não estão atualmente disponíveis para Linux VDA.

> A interface gráfica descrita neste artigo é a principal forma de usar o Scout. Alternativamente, você pode usar o PowerShell para configurar coletas e uploads de diagnóstico únicos ou agendados. Consulte Call Home.

Onde executar o Scout:

- Em uma implantação local, execute o Scout a partir de um Delivery Controller™ para capturar diagnósticos ou executar verificações em um ou mais Virtual Delivery Agents (VDAs), Delivery

Controllers, servidores StoreFront e License Servers. Você também pode executar o Scout a partir de um VDA para coletar diagnósticos locais.

- Em um ambiente Citrix Cloud que usa Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), execute o Scout a partir de um VDA para coletar diagnósticos locais.

O log do aplicativo Scout é armazenado em `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Este arquivo pode ser usado para solução de problemas.

### O que é coletado

Os diagnósticos coletados pelo Scout incluem arquivos de log de rastreamento do Citrix Diagnostic Facility (CDF). Um subconjunto de rastreamentos CDF chamado Always-on Tracing (AOT) também está incluído. As informações do AOT podem ser úteis para solucionar problemas comuns, como registros de VDA e inicializações de aplicativos/desktops. Nenhuma outra informação de Event Tracing for Windows (ETW) é coletada.

A coleta inclui:

- Entradas de registro criadas pelo Citrix Virtual Apps and Desktops em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informações do Windows Management Instrumentation (WMI) no **Citrix namespace**.
- Processos em execução.
- Dumps de falha de processos Citrix que são armazenados em `%PROGRAMDATA%\Citrix\CDF`.
- Informações de política Citrix, em formato CSV.
- Informações de instalação e atualização. A coleta pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront, logs de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

Sobre as informações de rastreamento:

- As informações de rastreamento são compactadas à medida que são coletadas, mantendo uma pequena pegada na máquina.
- Em cada máquina, o Citrix Telemetry Service mantém informações de rastreamento recentes compactadas por um máximo de oito dias.

- A partir do Citrix Virtual Apps and Desktops 7 1808, os rastreamentos AOT são salvos no disco local por padrão. (Em versões anteriores, os rastreamentos eram mantidos na memória.) Caminho padrão = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partir do Citrix Virtual Apps and Desktops 7 1811, os rastreamentos AOT salvos em compartilhamentos de rede são coletados com outros diagnósticos.
- Você pode modificar o tamanho máximo (padrão = 10 MB) e a duração do segmento, usando o cmdlet `Enable-CitrixTrace` ou a cadeia de caracteres do registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Os rastreamentos são anexados ao arquivo até que o arquivo atinja 10% de `MaxSize`.

Para obter uma lista dos pontos de dados que o Scout coleta, consulte Pontos de dados chave do Call Home.

### Configuração do Scout

O Scout pode ser configurado para funcionar em VDAs Linux. Para obter mais informações sobre VDA Linux e telemetria, consulte Integrar com o Serviço de Telemetria Citrix

O VDA Linux pode alterar automaticamente a porta do socket `ctxtelemetry` ou a porta para o serviço de telemetria. Se isso acontecer, você deve configurar a porta manualmente.

1. navegar para C:\Program Files\Citrix\Telemetry Service
2. Abra o arquivo ScoutUI.exe.config.
3. Altere o valor de LinuxVDATelemetryServicePort ou LinuxVDATelemetryWakeupPort para o que foi configurado no VDA Linux:

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. Salve as alterações e feche o arquivo.
2. Abra o Scout novamente para garantir que ele carregue a configuração mais recente.

### Sobre verificações de integridade

Os dados de verificação de integridade são armazenados em pastas em `C:\ProgramData\Citrix\TelemetryService\`.

### Verificações de integridade do site

As verificações de integridade do site estão incluídas no Serviço de Teste de Ambiente, que fornece uma avaliação abrangente dos serviços da Arquitetura de Gerenciamento FlexCast (FMA). Além de verificar a disponibilidade do serviço, essas verificações procuram outros indicadores de integridade, como conexões de banco de dados.

As verificações de integridade do site são executadas nos Delivery Controllers. Dependendo do tamanho do seu site, essas verificações podem levar até uma hora para serem concluídas.

#### VERIFICAÇÕES DE CONFIGURAÇÃO DO DELIVERY CONTROLLER

Como parte das verificações de integridade do site. As verificações de configuração do Delivery Controller verificam se os seguintes problemas existem, com base nas recomendações da Citrix para sites do Virtual Apps and Desktops:

- Um ou mais Delivery Controllers estão em um estado de falha.
- Há apenas um Delivery Controller no site.
- Os Delivery Controllers são de versões diferentes.

Além de atender às permissões e requisitos para verificações de integridade, as verificações de configuração do Delivery Controller exigem:

- Pelo menos um Controller ligado.
- O Serviço Broker em execução em um Controller.
- Uma conexão funcional do Controller com o banco de dados do site.

### Verificações de integridade do VDA

As verificações de integridade do VDA identificam possíveis causas para problemas comuns de registro do VDA, inicialização de sessão e redirecionamento de fuso horário.

Para registro no VDA, o Scout verifica:

- Instalação do software VDA
- Associação do domínio da máquina VDA
- Disponibilidade da porta de comunicação do VDA
- Status do serviço VDA
- Configuração do firewall do Windows
- Comunicação com o Controller
- Sincronização de tempo com o Controller

- Status de registro do VDA

Para inicializações de sessão em VDAs, o Scout verifica:

- Disponibilidade da porta de comunicação para inicialização de sessão
- Status dos serviços de inicialização de sessão
- Configuração do firewall do Windows para inicialização de sessão
- Licenças de Acesso de Cliente dos Serviços de Área de Trabalho Remota do VDA
- Caminho de inicialização do aplicativo VDA
- Configurações de registro para inicialização de sessão

Para redirecionamento de fuso horário em VDAs, o Scout verifica:

- Instalação de hotfix do Windows
- Instalação de hotfix do Citrix
- Configurações de política de grupo da Microsoft
- Configurações de política de grupo do Citrix

Para o Profile Management em VDAs, o Scout verifica:

- Detecção de hipervisor
- Detecção de provisionamento
- Citrix Aplicativos Virtuais e Desktops
- Configuração do vDisk pessoal
- Repositório de usuário
- Detecção do status do serviço Profile Management
- Teste de hooking do Winlogon.exe

Para executar verificações no Profile Management, você deve instalar e habilitar o Profile Management no VDA. Para obter mais informações sobre as verificações de configuração do Profile Management, consulte o artigo da Central de Conhecimento CTX132805.

**Verificações de integridade do StoreFront**

As verificações do StoreFront verificam o seguinte:

- O serviço Citrix Default Domain está em execução
- O serviço Citrix Credential Wallet está em execução

- Conexão do servidor StoreFront com o Active Directory na porta 88
- Conexão do servidor StoreFront com o Active Directory na porta 389
- A URL base tem um FQDN válido
- O endereço IP correto da URL base pode ser recuperado
- O pool de aplicativos do IIS está usando .NET 4.0
- Se o certificado está vinculado à porta SSL para a URL do host
- Se a cadeia de certificados está completa
- Se os certificados expiraram
- Se um certificado está prestes a expirar (em até 30 dias)

**Verificações do Servidor de Licenças**

As verificações do Servidor de Licenças verificam:

- Conexão do Servidor de Licenças a partir do Delivery Controller
- Status de acesso remoto do firewall do Servidor de Licenças
- Status do serviço de Licenciamento Citrix
- Estado do período de carência do Servidor de Licenças
- Conexão das portas do Servidor de Licenças
- Se o daemon do fornecedor Citrix (CITRIX) está em execução
- Se os relógios do sistema estão sincronizados
- Se o serviço de Licenciamento Citrix está sendo executado sob a conta de Serviço Local
- Presença do arquivo `CITRIX.opt`
- Data de elegibilidade dos Serviços de Sucesso do Cliente
- Atualização do Servidor de Licenças Citrix
- Se o certificado do Servidor de Licenças está no armazenamento raiz confiável do Delivery Controller

Além de atender às permissões e requisitos para verificações de integridade, o Servidor de Licenças deve estar associado a um domínio. Caso contrário, o Servidor de Licenças não é descoberto.

### Executar verificações de integridade

O procedimento de Verificação de Integridade compreende a seleção de máquinas, o início da verificação e, em seguida, a revisão do relatório de resultados.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Verificação de Integridade**.
2. Selecione as máquinas. Clique em **Localizar máquina** para descobrir máquinas. A página **Selecionar máquinas** lista todos os VDAs, Delivery Controllers e Servidores de Licenças descobertos no site. Você pode filtrar a exibição pelo nome da máquina. Marque a caixa de seleção ao lado de cada máquina da qual deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

   Para adicionar outros tipos de componentes (como servidores StoreFront e máquinas VDA), consulte Adicionar máquinas manualmente e Importar máquinas VDA. Não é possível adicionar manualmente Servidores Citrix Provisioning™ ou Servidores de Licenças.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar, uma mensagem será exibida na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

   - Resolver o problema e, em seguida, selecionar novamente a caixa de seleção da máquina. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (deixe sua caixa de seleção desmarcada). As verificações de integridade não são executadas para essa máquina.

   Quando os testes de verificação forem concluídos, clique em **Continuar**.
3. Execute as verificações de integridade nas máquinas selecionadas. O resumo lista as máquinas onde os testes são executados (as máquinas que você selecionou e que passaram nos testes de verificação). Clique em **Iniciar Verificação**.

   Durante e após a verificação:

   - A coluna **Status** indica o estado de verificação atual de uma máquina.
   - Para interromper todas as verificações em andamento, clique em **Parar Verificação** no canto inferior direito da página. (Você não pode cancelar a verificação de integridade de uma única máquina, apenas de todas as máquinas selecionadas. As informações das máquinas que concluíram as verificações são mantidas.

- Quando as verificações forem concluídas para todas as máquinas selecionadas, o botão **Parar Verificação** no canto inferior direito muda para **Concluído**.
- Se uma verificação falhar, você pode clicar em **Tentar Novamente** na coluna **Ação**.
- Se uma verificação for concluída sem problemas encontrados, a coluna **Ação** estará vazia.
- Se uma verificação encontrar problemas, clique em **Ver Detalhes** para mostrar os resultados.
- Após a conclusão da verificação para todas as máquinas selecionadas, não clique em **Voltar**. (Se você fizer isso, os resultados da verificação serão perdidos.)

4. Quando as verificações forem concluídas, clique em **Concluído** para retornar à página inicial do Scout.

#### Resultados da verificação de integridade

Para verificações Citrix que geram relatórios, os relatórios contêm:

- Hora e data em que o relatório de resultados foi gerado
- Máquinas que foram verificadas
- Condições que a verificação procurou nas máquinas de destino

### Permissões e requisitos

Permissões:

- Para coletar diagnósticos:
  - Você deve ser um administrador local e usuário de domínio para cada máquina da qual você está coletando diagnósticos.
  - Você deve ter permissão para gravar no diretório LocalAppData em cada máquina.
- Para executar verificações de integridade:
  - Você deve ser um membro do grupo de usuários do domínio.
  - Você deve ser um administrador completo ou ter uma função personalizada com permissões somente leitura e **Executar Testes de Ambiente** para o site.
  - Defina a política de execução de script para pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** outros privilégios de execução de script também podem funcionar.
- Use **Executar como administrador** ao iniciar o Scout.

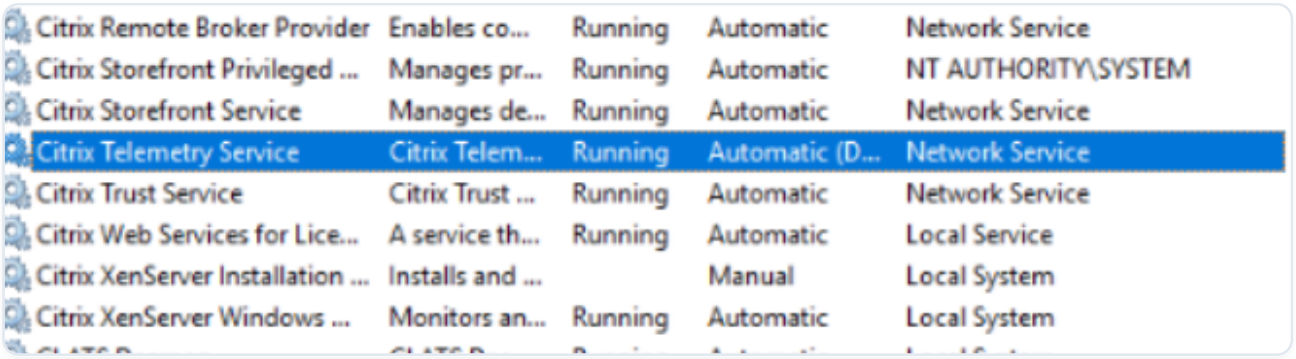
Para cada máquina da qual você coleta diagnósticos ou executa verificações de integridade:

- O Scout deve ser capaz de se comunicar com a máquina.
- O compartilhamento de arquivos e impressoras deve estar ativado.
- PSRemoting e WinRM devem estar habilitados. A máquina também deve estar executando o PowerShell 3.0 ou posterior.
- O Serviço de Telemetria Citrix deve estar em execução na máquina.
- O acesso à Windows Management Infrastructure (WMI) deve estar habilitado na máquina.
- Para definir um agendamento para a coleta de diagnóstico, a máquina deve estar executando uma versão compatível do Scout.

Não use o cifrão ($) em nomes de usuário especificados em nomes de caminho. Isso impede a coleta de informações de diagnóstico.

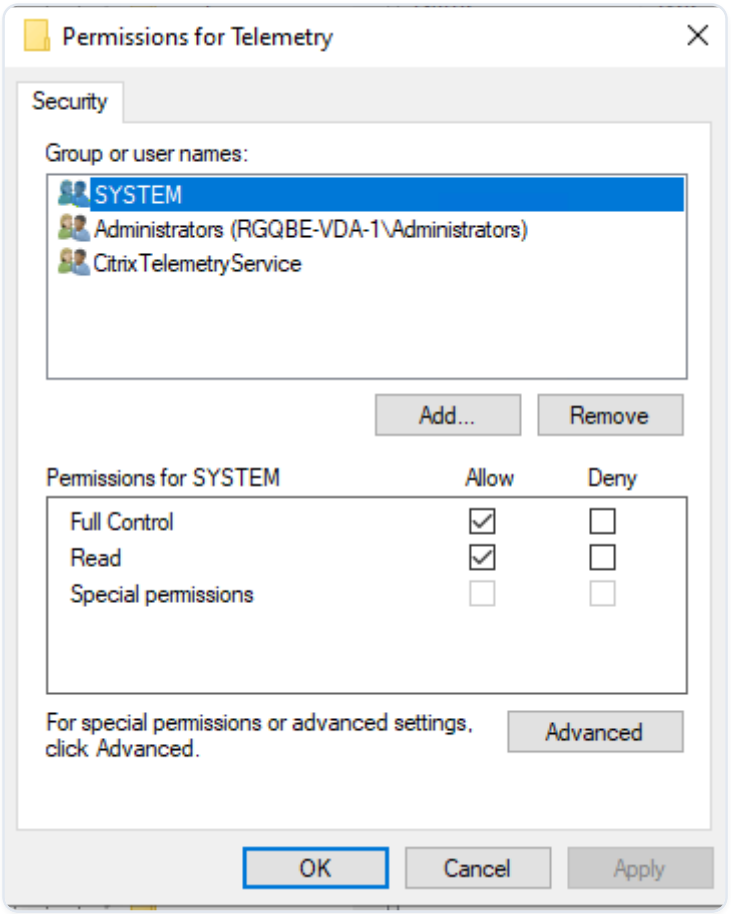
O Scout executa testes de verificação nas máquinas que você seleciona, para garantir que esses requisitos sejam atendidos.

O Serviço de Telemetria para Windows é executado no Serviço de Rede.

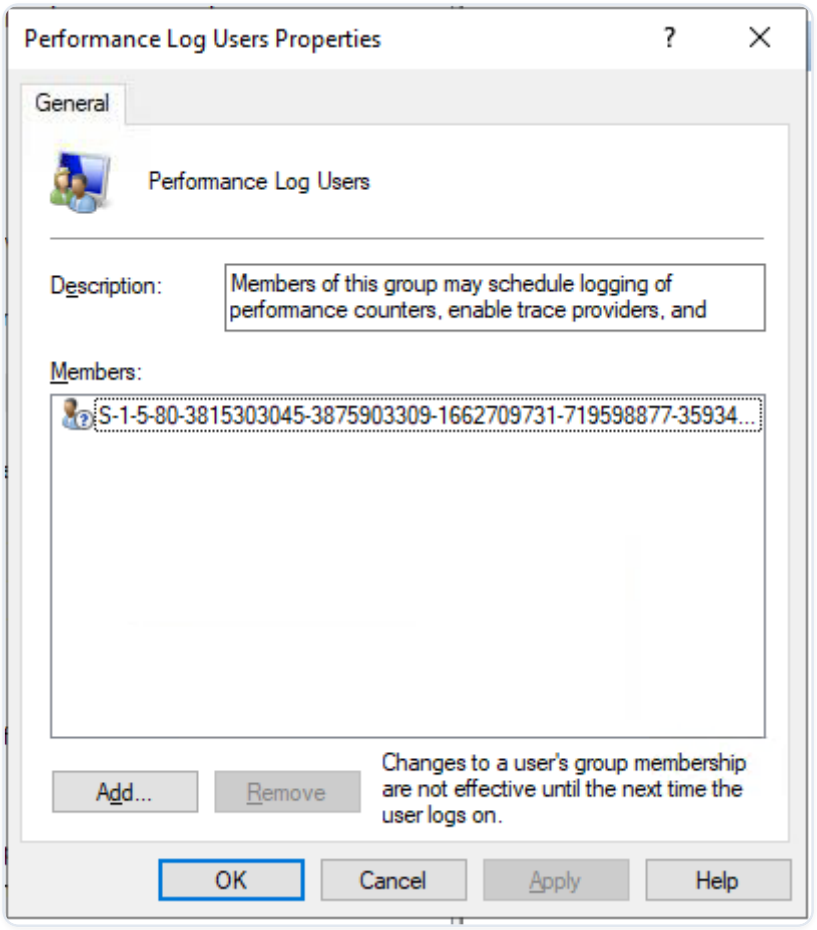



A Pasta de Rastreamento AOT é salva em `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Somente usuários no grupo Administrador, Sistema e SID do Serviço de Telemetria têm permissão para acessar o registro `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.




O SID do Serviço de Telemetria permanece no grupo Usuários do Log de Desempenho após a desinstalação do Serviço de Telemetria, mas você pode removê-lo manualmente.




### Testes de verificação

Antes de iniciar uma coleta de diagnóstico ou verificação de integridade, testes de verificação são executados automaticamente para cada máquina selecionada. Esses testes garantem que os requisitos sejam atendidos. Se um teste falhar para uma máquina, o Scout exibirá uma mensagem com ações corretivas sugeridas.

- **O Scout não consegue alcançar esta máquina** - Certifique-se de que:
  - A máquina está ligada.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)
  - O compartilhamento de arquivos e impressoras está ativado. Consulte a documentação da Microsoft para obter instruções.
- **Habilitar PSRemoting e WinRM** - Você pode habilitar o PowerShell remoting e o WinRM ao mesmo tempo. Usando **Executar como administrador**, execute o cmdlet `Enable-PSRemoting`. Para obter detalhes, consulte a ajuda da Microsoft para o cmdlet.
- **Scout requer PowerShell 3.0 (mínimo)** - Instale o PowerShell 3.0 (ou posterior) na máquina e, em seguida, habilite o PowerShell remoting.

- **Não é possível acessar o diretório LocalAppData nesta máquina** - Certifique-se de que a conta tenha permissão para gravar no diretório LocalAppData na máquina.
- **Não é possível localizar o Serviço de Telemetria Citrix** - Certifique-se de que o Serviço de Telemetria Citrix esteja instalado e iniciado na máquina.
- **Não é possível obter o agendamento** - Atualize a máquina para (mínimo) XenApp e XenDesktop 7.14.
- **WMI não está em execução na máquina** - Certifique-se de que o acesso ao Windows Management Instrumentation (WMI) esteja habilitado.
- **Conexões WMI bloqueadas** - Habilite o WMI no serviço Firewall do Windows.
- **Versão mais recente do Serviço de Telemetria Citrix necessária** - (A versão é verificada apenas para Coletar e Rastrear e Reproduzir.) Atualize a versão do Serviço de Telemetria na máquina (consulte Instalar e atualizar). Se você não atualizar o serviço, essa máquina não será incluída nas ações de **Coletar** ou **Rastrear e Reproduzir**.
- **Scout não consegue se conectar ao socket systemd nesta máquina** - Certifique-se de que:
  - A porta 7503 está aberta. Verifique se o ctxtelemetry.socket do systemd está escutando na porta 7503 na máquina. A porta pode ser diferente se a porta do ctxtelemetry.socket tiver sido alterada. Consulte Configuração do Scout para ajustar as portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)
- **O Serviço de Telemetria Linux VDA não está iniciado nesta máquina** - Certifique-se de que:
  - A porta 7502 está aberta. Verifique se o Serviço de Telemetria do Linux VDA está instalado e iniciado na máquina. A porta pode ser diferente se a porta do serviço de telemetria tiver sido alterada. Consulte Configuração do Scout para ajustar as portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)

### Compatibilidade de versão

Esta versão do Scout (3.x) destina-se a ser executada em Controladores e VDAs do Citrix Virtual Apps and Desktops (ou no mínimo XenApp e XenDesktop 7.14).

| Recurso | Scout 2.23 | Scout 3.0 | --- | --- | ---| -- | Suporta Citrix Virtual Apps and Desktops (além de XenApp e XenDesktop 7.14 a 7.18) | Sim | Sim Suporta XenDesktop 5.x, 7.1–7.13 | Sim | Não

Suporta XenApp 6.x, 7.5 a 7.13 | Sim | Não Entregue com o produto | 7.1–7.13 | A partir de 7.14 Pode ser baixado do artigo CTX | Sim | Não Capturar rastreamentos CDF | Sim | Sim Capturar rastreamentos Always-on (AOT) | Não | Sim Permitir a coleta de dados de diagnóstico | Até 10 máquinas por vez (por padrão) | Ilimitado (sujeito à disponibilidade de recursos) Permitir que dados de diagnóstico sejam enviados para a Citrix | Sim | Sim Permitir que dados de diagnóstico sejam salvos localmente | Sim | Sim Suporte a credenciais do Citrix Cloud™ | Não | Sim Suporte a credenciais da Citrix | Sim | Sim Suporte a servidor proxy para uploads | Sim | Sim Ajustar agendamentos | N/A | Sim Suporte a scripts | Linha de comando (somente Controller local) | PowerShell usando cmdlets Call Home (qualquer máquina com o Serviço de Telemetria instalado) Verificações de integridade | Não | Sim Mascaramento de Dados | Não | A partir da versão 3.17

### Instalar e atualizar

Por padrão, o Scout é instalado ou atualizado automaticamente como parte do Serviço de Telemetria Citrix quando você instala ou atualiza um VDA ou um Controller.

Se você omitir o Serviço de Telemetria Citrix ao instalar um VDA, ou remover o serviço posteriormente, execute `TelemetryServiceInstaller_xx.msi` da pasta `x64\Virtual Desktop Components` ou `x86\Virtual Desktop Components` na mídia de instalação do Citrix Virtual Apps and Desktops.

Ao selecionar a ação **Coletar** ou **Rastrear e Reproduzir**, você será notificado se uma máquina estiver executando uma versão mais antiga do Serviço de Telemetria Citrix. A Citrix recomenda usar a versão mais recente suportada. Se você não atualizar o Serviço de Telemetria nessa máquina, ele não será incluído nas ações **Coletar** ou **Rastrear e Reproduzir**. Para atualizar o Serviço de Telemetria, use o mesmo procedimento de instalação.

### Autorização de upload

Se você planeja fazer upload de coleções de diagnóstico para a Citrix, você deve ter uma conta Citrix ou Citrix Cloud. (Estas são as credenciais que você usa para acessar downloads da Citrix ou acessar o Citrix Cloud Control Center.) Após a validação das credenciais da sua conta, um token é emitido.

Se você autenticar com uma conta Citrix ou uma conta Citrix Cloud, clique em um link para acessar o Citrix Cloud usando HTTPS com seu navegador padrão. Depois de inserir suas credenciais do Citrix Cloud, o token é exibido. Copie o token e cole-o no Scout. Você pode então continuar no assistente do Scout.

O token é armazenado localmente na máquina onde você está executando o Scout. Para permitir o uso desse token na próxima vez que você executar **Coletar** ou **Rastrear e Reproduzir**, selecione a caixa de seleção **Armazenar token e pular esta etapa no futuro**.

Você deve reautorizar cada vez que selecionar **Agendar** na página inicial do Scout. Você não pode usar um token armazenado ao criar ou alterar um agendamento.

#### Usar um proxy para uploads

Se você deseja usar um servidor proxy para fazer upload de coleções para a Citrix, pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Alternativamente, você pode especificar o endereço IP e o número da porta do servidor proxy.

### Localizar máquina

Para os procedimentos **Coletar**, **Rastrear e Reproduzir** e **Agendar**, o Scout lista os Controllers e VDAs que ele descobre automaticamente.

Ao executar Scout Health Check a partir do Delivery Controller, clique em **Localizar máquina** para descobrir máquinas, incluindo delivery controllers, VDAs, servidores de licença e servidores StoreFront.

Ao executar o Scout Health Check a partir de uma máquina ingressada no domínio que não é um Delivery Controller, o Scout não consegue descobrir máquinas automaticamente. Você precisa adicionar máquinas manualmente ou importar máquinas VDA.

### Adicionar máquinas manualmente

Depois que o Scout lista os Controladores e VDAs que ele descobre, você pode adicionar manualmente outras máquinas na implantação, como servidores StoreFront, Servidores de Licença e servidores Citrix Provisioning.

Ao executar verificações de integridade:

- Os Servidores de Licença Citrix no domínio são descobertos automaticamente. Você não pode adicionar Servidores de Licença manualmente.
- As verificações de integridade não oferecem suporte atualmente a servidores Citrix Provisioning.

Em qualquer página do Scout que liste as máquinas descobertas, clique em **+ Adicionar máquina**. Digite o FQDN da máquina que você deseja adicionar e, em seguida, clique em

**Continuar**. Repita para adicionar outras máquinas, conforme necessário. (Embora inserir um alias DNS em vez de um FQDN possa parecer válido, as verificações de integridade podem falhar.)

As máquinas adicionadas manualmente sempre aparecem no topo da lista de máquinas, acima das máquinas descobertas.

Uma maneira fácil de identificar uma máquina adicionada manualmente é o botão vermelho de exclusão na extremidade direita da linha. Somente as máquinas adicionadas manualmente têm esse botão. As máquinas descobertas não têm.

Para remover uma máquina adicionada manualmente, clique no botão vermelho na extremidade direita da linha. Confirme a exclusão. Repita para excluir outras máquinas adicionadas manualmente.

O Scout lembra as máquinas adicionadas manualmente até que você as remova. Quando você fecha e reabre o Scout, as máquinas adicionadas manualmente ainda estão listadas no topo da lista.

Os rastreamentos CDF não são coletados ao usar **Rastrear e Reproduzir** em servidores StoreFront. No entanto, todas as outras informações de rastreamento são coletadas.

### Importar máquinas VDA

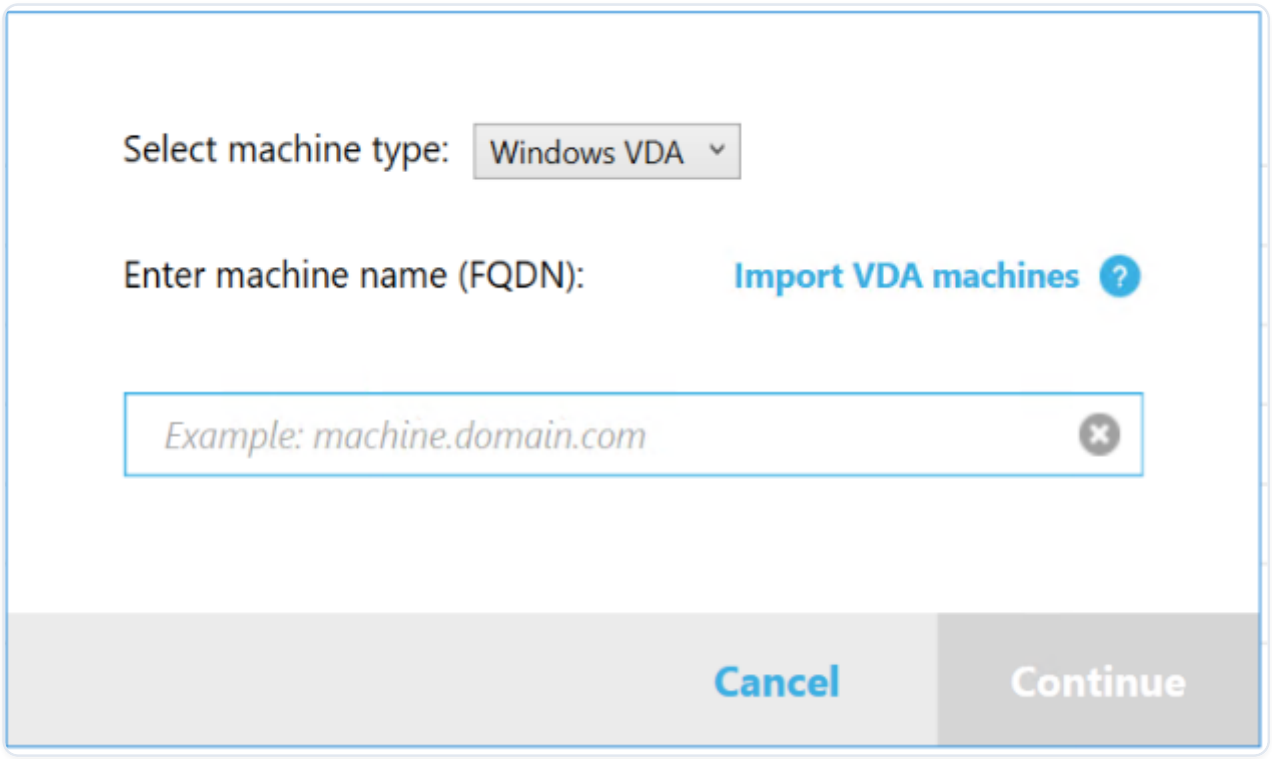
Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

1. No Delivery Controller ou Connector, gere o arquivo da lista de máquinas com o comando PowerShell. No Connector, você deve inserir as credenciais Citrix e selecionar o cliente na caixa de diálogo pop-up.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. Copie o arquivo machineList.txt para a máquina ingressada no domínio na qual você deseja iniciar o Scout Health Check.
3. Na página de Verificação de Integridade do Scout, clique em **Adicionar Máquina**.
4. Selecione o tipo de máquina **Windows VDA**.
5. Clique em **Importar máquinas VDA**.
6. Selecione o arquivo machineList.txt.
7. Clique em **Abrir**.

As máquinas VDA importadas são listadas na página de Verificação de Integridade do Scout.




### Coletar diagnósticos

O procedimento de **Coleta** consiste em selecionar máquinas, iniciar a coleta de diagnósticos e, em seguida, carregar o arquivo contendo a coleta para a Citrix ou salvá-lo localmente.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página inicial, clique em **Coletar**.
2. Selecionar máquinas.

   - Em um Controller, a página **Selecionar máquinas** lista todos os VDAs e Controllers no site. Você pode filtrar a exibição por nome da máquina. Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.
   - Em outros componentes (como servidores VDA), a página **Selecionar máquinas** lista apenas a máquina local. A adição manual de máquinas não é suportada.

   Marque a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar, uma mensagem será exibida na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolva o problema e então selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignore essa máquina (deixe sua caixa de seleção desmarcada). Os diagnósticos não serão coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

3. Coletar diagnósticos. O resumo lista todas as máquinas das quais os diagnósticos são coletados (as máquinas que você selecionou e que passaram nos testes de verificação). Clique em **Iniciar Coleta**.

   Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta para uma máquina.
   - Para interromper uma coleta em andamento em uma única máquina, clique em **Cancelar** na coluna **Ação** para essa máquina.
   - Para interromper todas as coletas em andamento, clique em **Parar Coleta** no canto inferior direito da página. Os diagnósticos das máquinas que concluíram a coleta são mantidos. Para retomar a coleta, clique em **Tentar Novamente** na coluna **Ação** para cada máquina.
   - Quando a coleta for concluída para todas as máquinas selecionadas, o botão **Parar Coleta** no canto inferior direito muda para **Continuar**.
   - Para coletar diagnósticos novamente, clique em **Coletar Novamente** na coluna **Ação** dessa máquina. A coleta mais recente sobrescreve a anterior.
   - Se uma coleta falhar, você pode clicar em **Tentar Novamente** na coluna **Ação**. Somente coletas bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Voltar**. (Se você clicar, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

4. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo na máquina local.

   Se você optar por carregar o arquivo agora, continue com a Etapa 5.

   Se você optar por salvar o arquivo localmente:

   - Uma caixa de diálogo **Salvar** do Windows é exibida. navegar até o local desejado.

- Quando o salvamento local for concluído, o nome do caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Você pode fazer o upload do arquivo mais tarde para a Citrix. Consulte CTX136396.

Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir nenhuma outra etapa neste procedimento.

5. autenticar para uploads e, opcionalmente, especifique um proxy. Para obter detalhes, consulte Autorização de upload.

   - Se você não se autenticou através do Scout, continue com esta etapa.
   - Se você se autenticou através do Scout, o token de autorização armazenado é usado por padrão. Se é isso que você deseja fazer, selecione esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleta. Continue com a Etapa 6.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as propriedades de internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será iniciado em uma página do Citrix Cloud onde um token é exibido. Copie o token e cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

6. Insira informações sobre o upload.

   - O campo nome contém o nome padrão para o arquivo dos diagnósticos coletados. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo nome vazio, o nome padrão será usado.)
   - Opcionalmente, especifique um número de caso de suporte da Citrix de 8 dígitos.

- No campo opcional **Descrição**, descreva o problema e indique quando o problema ocorreu, se aplicável.

Quando terminar, clique em **Iniciar Carregamento**.

Durante o carregamento, a parte inferior esquerda da página aproxima a porcentagem do carregamento que foi concluída. Para cancelar um carregamento em andamento, clique em **Parar Carregamento**.

Quando o carregamento for concluído, o URL de sua localização será exibido e vinculado. Você pode seguir o link para o local da Citrix para visualizar a análise do carregamento, ou pode copiar o link.

Clique em **Concluído** para retornar à página inicial do Scout.

### Rastrear e reproduzir

O procedimento **Rastrear e Reproduzir** compreende selecionar máquinas, iniciar um rastreamento, reproduzir problemas, concluir a coleta de diagnósticos e, em seguida, carregar o arquivo para a Citrix ou salvá-lo localmente.

Este procedimento é semelhante ao procedimento padrão de **Coleta**. No entanto, ele permite que você inicie um rastreamento em máquinas e, em seguida, recrie problemas nessas máquinas. Todas as coletas de diagnóstico incluem informações de rastreamento AOT. Este procedimento adiciona rastreamentos CDF para ajudar na solução de problemas.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página inicial, clique em **Rastrear e Reproduzir**.
2. Selecione as máquinas. A página **Selecionar máquinas** lista todos os VDAs e Controladores no site. Você pode filtrar a exibição por nome da máquina. Selecione a caixa de seleção ao lado de cada máquina da qual deseja coletar rastreamentos e diagnósticos. Em seguida, clique em **Continuar**.

   Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será publicada na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolver o problema e, em seguida, selecionar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Pule essa máquina (deixe sua caixa de seleção desmarcada). Diagnósticos e rastreamentos não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

3. Inicie o rastreamento. O resumo lista todas as máquinas das quais os rastreamentos são coletados. Clique em **Iniciar Rastreamento**.

   Em uma ou mais das máquinas selecionadas, reproduza os problemas que você encontrou. A coleta de rastreamento continua enquanto você faz isso. Quando terminar de reproduzir o problema, clique em **Continuar** no Scout. Isso interrompe o rastreamento.

   Depois de interromper o rastreamento, indique se você reproduziu o problema durante o rastreamento.

4. Colete diagnósticos das máquinas. Clique em **Iniciar Coleta**. Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta para uma máquina.
   - Para interromper uma coleta em andamento em uma única máquina, clique em **Cancelar** na coluna **Ação** para essa máquina.
   - Para interromper todas as coletas em andamento, clique em **Parar Coleta** no canto inferior direito da página. Os diagnósticos das máquinas que concluíram a coleta são mantidos. Para retomar a coleta, clique em **Tentar Novamente** na coluna **Ação** para cada máquina.
   - Quando a coleta for concluída para todas as máquinas selecionadas, o botão **Parar Coleta** no canto inferior direito muda para **Continuar**.
   - Para coletar diagnósticos novamente de uma máquina, clique em **Coletar Novamente** na coluna **Ação** dessa máquina. A coleta mais recente sobrescreve a anterior.
   - Se uma coleta falhar, você pode clicar em **Tentar Novamente** na coluna **Ação**. Somente as coletas bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Voltar**. (Se você o fizer, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

5. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo localmente.

   Se você optar por carregar o arquivo agora, continue com a Etapa 6.

Se você optar por salvar o arquivo localmente:

- Uma caixa de diálogo Salvar do Windows é exibida. Selecione o local desejado.
- Quando o salvamento local for concluído, o caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Lembre-se: Você pode carregar o arquivo mais tarde do Citrix; consulte CTX136396 para Citrix Insight Services.

Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir mais nenhuma etapa neste procedimento.

6. autenticar para uploads e, opcionalmente, especifique o proxy. Revise Autorização de upload para obter detalhes deste processo.

   - Se você não se autenticou através do Scout, continue com esta etapa.
   - Se você se autenticou através do Scout, o token de autorização armazenado é usado por padrão. Se é isso que você deseja fazer, escolha esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleção. Continue com a Etapa 7.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será iniciado em uma página do Citrix Cloud onde um token é exibido. Copie o token e, em seguida, cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

7. Forneça informações sobre o upload.

   Insira os detalhes do upload:

- O campo de nome contém o nome padrão para o arquivo dos diagnósticos coletados. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo de nome vazio, o nome padrão será usado.)
- Opcionalmente, especifique um número de caso de Suporte Citrix de 8 dígitos.
- No campo opcional Descrição, descreva o problema e indique quando o problema ocorreu, se aplicável.

Quando terminar, clique em **Iniciar Upload**.

Durante o upload, a parte inferior esquerda da página aproxima a porcentagem do upload que foi concluída. Para cancelar um upload em andamento, clique em **Parar Upload**.

Quando o upload for concluído, o URL de sua localização será exibido e vinculado. Você pode seguir o link para o local da Citrix para visualizar a análise do upload, ou pode copiar o link.

Clique em **Concluído** para retornar à página inicial do Scout.

### Habilitar coleta de log adicional

A função **Habilitar coleta de log adicional** permite que você use a função de rastreamento e reprodução com mais ferramentas, como perfmon, Netsh, DebugView e Wireshark.

> **Nota:**
>
> Isso se aplica apenas a máquinas locais.

> Para configurar a coleta de log adicional:

1. Inicie o Citrix Scout.
2. Clique no ícone de engrenagem **Configurações**.
3. Clique em **Habilitar coleta de log adicional com mais ferramentas**.
4. Clique em **Salvar**.

Para coletar logs adicionais:

1. Na página inicial do Scout, clique em **Rastrear e Reproduzir**.
2. Na página **Selecionar máquinas**, clique na engrenagem no lado direito da máquina local.
3. Na página **Selecione as ferramentas necessárias para o registro:**, clique em **Baixar Ferramentas**.

4. Na página **Baixar Ferramentas**, selecione as ferramentas que deseja usar e clique em **Baixar**. As ferramentas são então baixadas, exceto o Wireshark. O Wireshark só pode ser baixado e instalado manualmente. Nota: Se você optar por baixar outras ferramentas manualmente, deverá extrair o conteúdo do arquivo .zip baixado para `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`. Por exemplo, se você baixar o arquivo DebugView.zip, descompactaria o conteúdo do arquivo para `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`.
5. Na página **Selecione as ferramentas necessárias para o registro:**, clique em **Atualizar Status**. Todas as ferramentas selecionadas aparecem como **Presente** na coluna Status.
6. Selecione as ferramentas para registro e clique em **Avançar**.
7. Siga as instruções de Rastrear e Reproduzir.
8. Após a conclusão, verifique os logs no arquivo zip. Os logs são compactados na pasta *CDCLogs*.

> **Nota:**
>
> Se a Ferramenta Procmon for selecionada para rastreamento, os logs do Process Monitor podem aumentar rapidamente. Certifique-se de selecionar apenas as ferramentas necessárias. Você também pode monitorar o tamanho dos logs em *%temp%\Scout-CDC-Log*.

### Agendar coletas

> **Nota:**
>
> Atualmente, você pode agendar coletas, mas não verificações de integridade.

> O procedimento de Agendamento compreende a seleção de máquinas e, em seguida, a configuração ou cancelamento do agendamento. As coletas agendadas são automaticamente carregadas para a Citrix. (Você pode salvar coletas agendadas localmente usando a interface do PowerShell. Consulte Citrix Call Home.)

1. Inicie o Scout. No menu Iniciar da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Agendar**.

2. Selecione as máquinas. Todos os VDAs e Controladores no site são listados. Você pode filtrar a exibição pelo nome da máquina.

   Ao instalar VDAs e Controladores usando a interface gráfica, se você definiu um agendamento do Call Home (consulte Citrix Call Home), o Scout exibe essas configurações por padrão. Você pode usar esta versão do Scout para iniciar coletas agendadas pela primeira vez ou para alterar um agendamento configurado anteriormente.

   Embora você tenha ativado/desativado o Call Home por máquina durante a instalação do componente, um agendamento configurado no Scout afeta todas as máquinas que você selecionar.

   Marque a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

   Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.

   O Scout inicia automaticamente testes de verificação em cada uma das máquinas selecionadas, garantindo que elas atendam aos critérios em Testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será exibida na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

   - Resolva o problema e, em seguida, selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (deixe sua caixa de seleção desmarcada). Diagnósticos (ou rastreamentos) não são coletados dessa máquina.

   Quando os testes de verificação forem concluídos, clique em **Continuar**.

   A página de resumo lista as máquinas às quais os agendamentos são aplicados. Clique em **Continuar**.

3. Defina o agendamento. Indique quando você deseja que os diagnósticos sejam coletados. Lembre-se: O agendamento afeta todas as máquinas selecionadas.

   - Para configurar um agendamento semanal para as máquinas selecionadas, clique em **Semanal**. Escolha o dia da semana. Insira a hora do dia (formato 24 horas) para o início da coleta.
   - Para configurar um agendamento diário para as máquinas selecionadas, clique em **Diário**. Insira a hora do dia (formato 24 horas) para o início da coleta.

- Para cancelar um agendamento existente para as máquinas selecionadas (e não substituí-lo por outro), clique em **Desativar**. Isso cancela qualquer agendamento que tenha sido configurado anteriormente para essas máquinas.

Clique em **Continuar**.

4. autenticar para uploads e, opcionalmente, especifique um proxy. Revise Autorização de upload para obter detalhes sobre este processo. Lembre-se: Você não pode usar um token armazenado para autenticar ao trabalhar com um agendamento do Scout.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**.

   Na página de credenciais:

   - Se você deseja usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será aberto em uma página do Citrix Cloud onde um token é exibido. Copie o token e, em seguida, cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

   Revise o agendamento configurado. Clique em **Concluído** para retornar à página inicial do Scout.

   Durante uma coleta, o log de aplicativos do Windows de cada máquina selecionada contém entradas sobre a coleta e o upload.

### Mascaramento de dados

As informações de diagnóstico coletadas usando o Citrix Scout podem conter informações sensíveis à segurança. O recurso de mascaramento de dados do Citrix Scout permite mascarar dados sensíveis em arquivos de diagnóstico antes de enviá-los para a Citrix.

O mascaramento de dados do Scout é configurado para mascarar o endereço IP, nomes de máquinas, nomes de domínio, nomes de usuário, nomes de hypervisor, nomes de Delivery Group, nomes de catálogo, nomes de aplicativos e SIDs.

> **Nota:**
>
> Os rastreamentos CDF são criptografados e não podem ser mascarados.
>
> Os logs do Linux VDA são compactados para o formato `.tar.gz2` e não podem ser mascarados.

### Coletar novos diagnósticos e realizar mascaramento de dados

Para usar o recurso de mascaramento de dados do Citrix Scout, inicie o Scout a partir da linha de comando.

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório onde o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie o Scout: `ScoutUI.exe datamasking`.
4. Clique em **Coletar** ou **Rastrear e Reproduzir** para coletar diagnósticos.
5. Após a conclusão da coleta, selecione **Habilitar mascaramento de dados**. Esta opção é habilitada por padrão.
6. Configure a máscara de dados. Você pode usar as regras padrão ou personalizar as regras.
7. Selecione se deseja carregar ou salvar a coleta de diagnósticos.
    - Se você selecionar **Carregar a coleta de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleta de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

### Executar mascaramento de dados em diagnósticos existentes

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório onde o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie o Scout diretamente no modo de mascaramento de dados: `ScoutUI.exe datamasking filePath`.
4. Selecione “Habilitar mascaramento de dados” para continuar. Esta opção é habilitada por padrão.

5. Configure a máscara de dados. Você pode executar o mascaramento de dados com as regras padrão ou personalizar as regras.
6. Selecione se deseja carregar ou salvar a coleção de diagnósticos.
    - Se você selecionar **Carregar a coleção de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleção de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

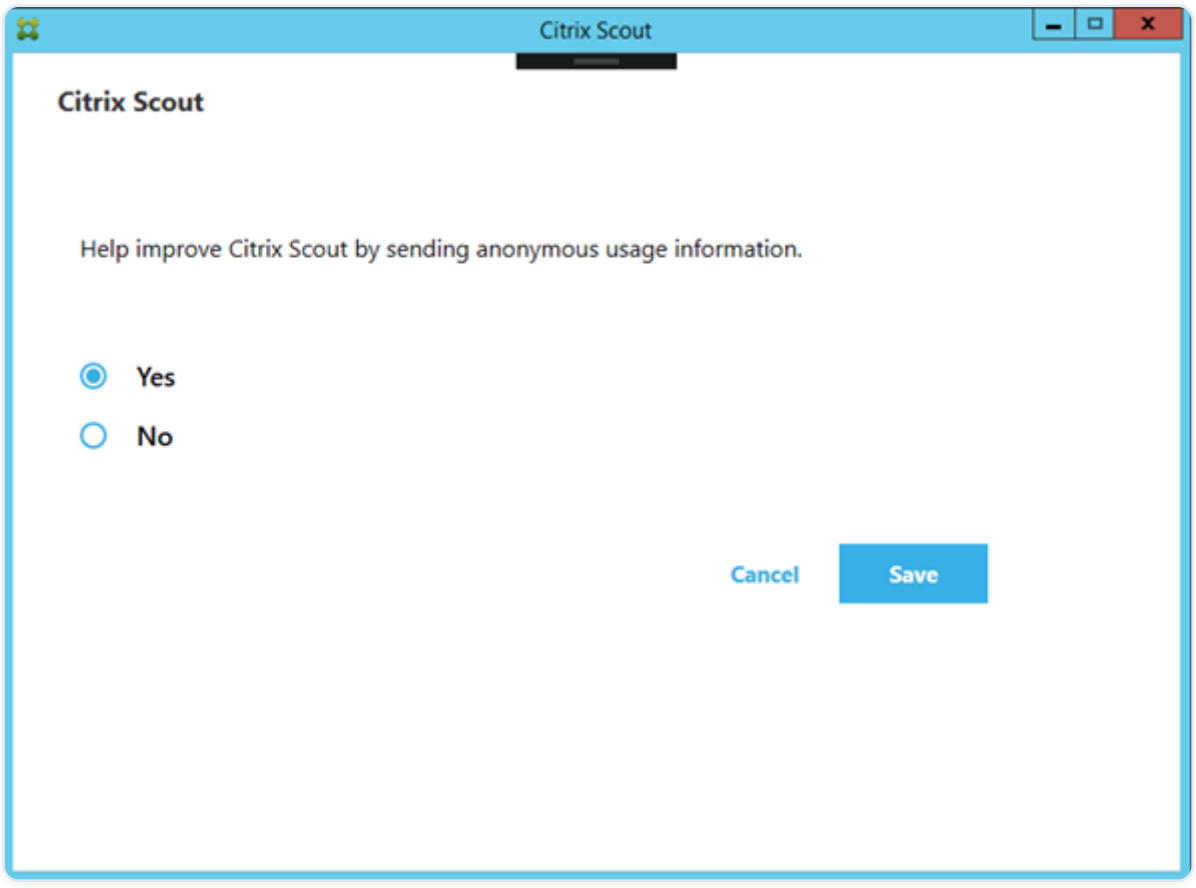
**Locais do arquivo de dados mascarados e do arquivo de mapeamento**

Depois de carregar ou salvar a coleção de diagnósticos, clique no link para abrir os diagnósticos originais e mascarados, e abra o arquivo de informações de mapeamento.

## Coleta de dados de uso

Ao usar o Scout, a Citrix usa o Google Analytics para coletar dados de uso anônimos a serem usados para futuros recursos e melhorias do produto. A coleta de dados é habilitada por padrão.

Para alterar a coleta e o upload de dados de uso, clique no ícone de engrenagem **Configurações** na interface do usuário do Scout. Você pode então escolher se deseja enviar as informações selecionando **Sim** ou **Não** e, em seguida, clicando em **Salvar**.



## Principais pontos de dados do Call Home

O Call Home coleta os seguintes pontos de dados principais.

(M) = Capturado apenas durante a coleta manual (cmdlet do PowerShell `Start-CitrixCallHomeUpload`)

| NOME DO ARQUIVO | CATEGORIA | GRUPO DE DADOS |
|---|---|---|
| | | |
| | | Máquinas |
| | | XDSite |
| | | Informações do Site |
| | | Informações do DB do Broker (M) |
| | | Versão do DB instalada (M) |
| | | Status do Serviço Broker (M) |
| | | Instâncias de Serviço Registradas (M) |
| | | Teste de Licença do Broker (M) |
| | | Sessão HDX™ Ativa (M) |
| | | Administrador do Broker |
| | | Permissão de Administrador do Broker |
| | | Configuração RDS (inclui LicensingSettings, SessionSettings, SpecifiedLicenseServers e RegisteredLicenseServers) |

| | | |
|---|---|---|
| | | Serviço de Monitoramento (M) (inclui MonitorConfiguration, MonitorDataStore, MonitorDBConnection, MonitorDBSchemaVersion, MonitorService, MonitorServiceAddedCapability, MonitorServiceInstance, MonitorServiceStatus e MonitorInstalledDBVersion) |
| | | Log de Configuração |
| | | Log de Conexão |
| | | Conexões de Hypervisor (M) |
| | | Conexão de Hypervisor do Broker |
| | | Alertas de Hypervisor |
| | | Catálogos |
| | | Agentes de SO de Múltiplas Sessões (M) |
| | | Agentes de SO de Sessão Única (M) |
| | | Aplicativos Publicados |
| | | Grupos de Entrega |
| | | Agentes de Entrega Configurados |

| | | |
|---|---|---|
| | | Componentes Citrix Instalados |

| | | |
|---|---|---|
| | | Informações do Serviço de Broker Citrix |
| | | Arquivo de configuração do Serviço de Broker |
| | | Arquivo de configuração do Machine Creation Services™ |
| | | Arquivo de configuração do Serviço de Host |
| | | Arquivo de configuração do Serviço de Identidade AD |
| | | Arquivo de configuração do Serviço de Configuração |
| | | Arquivo de configuração do Serviço de Registro de Configuração |
| | | Arquivo de configuração do Serviço de Administração Delegada |
| | | Arquivo de configuração do Serviço de Teste de Ambiente |
| | | Arquivo de configuração do Serviço de Monitoramento |
| | | Arquivo de configuração do Serviço Storefront™ |
| | | Arquivo de configuração do Agente da Estação de Trabalho |
| | | Informações do VDA Citrix |
| | | Hotfix XD Citrix |

| | | |
|---|---|---|
| | | Citrix_VirtualChannel_Graphics_Enum |
| | | Citrix_VirtualChannel_Flash_Enum |
| | | Citrix_VirtualChannel_Printer_Enum |

| | | |
|---|---|---|
| | | Computador |
| | | BIOS |
| | | Informações da Memória |
| | | Processador |
| | | Dispositivo PNP |
| | | Dispositivo |
| | | Unidade de Disco |
| | | Unidade Lógica |
| | | Uso do Arquivo de Paginação |
| | | Adaptador de Rede |
| | | Configuração do Adaptador de Rede |
| | | ipConfig |
| | | Controlador de Vídeo |
| | | Controlador IDE |
| | | Controlador SCSI |

| | | |
|---|---|---|
| | | HKLM: \Software\Wow6432Node\Citrix |
| | | HKLM: \System\CurrentControlSet\Control\Citrix |
| | | HKLM: \SOFTWARE\Policies\Citrix |
| | | HKLM: \Software\Microsoft\Cryptography |
| | | HKLM: \Software\Wow6432Node\Microsoft\Cryptography |
| | | HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Windows |
| | | HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon |
| | | HKLM: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| | | HKLM: \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| | | HKLM: \SYSTEM\CurrentControlSet\Control\Print\Environments |

| | | |
|---|---|---|
| | | HKLM:\System\CurrentControlSet\Control\Session Manager |
| | | HKLM:\System\CurrentControlSet\Control\Terminal Server |
| | | HKCU:\Control Panel\Desktop |
| | | HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\Windows |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation |

| | | |
|---|---|---|
| | | Driver |
| | | EnvVariables |
| | | SO |
| | | Processo |
| | | Serviço |

| | | |
|---|---|---|
| | | Service Pack |
| | | GPResult |
| | | Hotfix da Microsoft |
| | | Netstat |
| | | Driver PNP |

| | | |
|---|---|---|
| | | Log de Eventos do Sistema |
| | | AOT (Rastreamento Sempre Ativo) |
| | | Despejos de Memória |

| | | |
|---|---|---|
| | | tempo de atividade |
| | | memória |
| | | sistema de computador |
| | | processador |
| | | controlador de vídeo |
| | | unidade de disco |
| | | informações do navegador |
| | | tempos de reinicialização |
| | | uso de memória |
| | | uso de disco |
| | | resoluções de sessão ICA |
| | | profundidade de cor ICA |
| | | metainstaller-ceip-machine-id |

| | | |
|---|---|---|
| | | Contagem de Lojas |
| | | Contagem de Servidores no Grupo de Servidores |
| | | Contagem de Delivery Controller™ por Loja |
| | | HTTPS Habilitado |
| | | Experiência Clássica Habilitada para Citrix Receiver™ |
| | | Configuração do HTML5 Receiver para Citrix Receiver |
| | | Controle de Workspace Habilitado para Citrix Receiver |
| | | Acesso Remoto Habilitado para Loja |
| | | Contagem de Gateways |
| | | Serviço JSON explícito para autenticação integrada do NetScaler® |

# Administração delegada

**Nota:**

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

O modelo de administração delegada oferece a flexibilidade para corresponder à forma como sua organização deseja delegar atividades de administração, usando controle baseado em função e objeto. A administração delegada acomoda implantações de todos os tamanhos e permite configurar maior granularidade de permissões à medida que sua implantação cresce em complexidade. A administração delegada usa três conceitos: administradores, funções e escopos.

- **Administradores:** Um administrador representa uma pessoa individual ou um grupo de pessoas identificadas por sua conta do Active Directory. Cada administrador está associado a um ou mais pares de função e escopo.
- **Funções:** Uma função representa uma função de trabalho e tem permissões definidas associadas a ela. Por exemplo, a função de Administrador de Grupo de Entrega tem permissões como 'Criar Grupo de Entrega' e 'Remover Desktop do Grupo de Entrega'. Um administrador pode ter várias funções para um site, então uma pessoa pode ser um Administrador de Grupo de Entrega e um Administrador de Catálogo de Máquinas. As funções podem ser integradas ou personalizadas.

  As funções integradas são:

| FUNÇÃO | PERMISSÕES |
|---|---|
| Administrador Completo | Pode executar todas as tarefas e operações. Um Administrador Completo é sempre combinado com o escopo Todos. |
| Administrador Somente Leitura | Pode ver todos os objetos em escopos especificados, além de informações globais, mas não pode alterar nada. Por exemplo, um Administrador Somente Leitura com Escopo=Londres pode ver todos os objetos globais (como Registro de Configuração) e quaisquer objetos com escopo de Londres (por exemplo, Grupos de Entrega de Londres). No entanto, esse administrador não pode ver objetos no escopo de Nova York (assumindo que os escopos de Londres e Nova York não se sobreponham). |
| Administrador de Help Desk | Pode visualizar Grupos de Entrega e gerenciar as sessões e máquinas associadas a esses grupos. Pode ver o |

| FUNÇÃO | PERMISSÕES |
| --- | --- |
| | Catálogo de Máquinas e as informações do host para os Grupos de Entrega que estão sendo monitorados. Também pode realizar operações de gerenciamento de sessão e gerenciamento de energia da máquina para as máquinas nesses Grupos de Entrega. |
| Administrador de Catálogo de Máquinas | Pode criar e gerenciar Catálogos de Máquinas e provisionar as máquinas neles. Pode construir Catálogos de Máquinas a partir da infraestrutura de virtualização, Provisioning Services e máquinas físicas. Esta função pode gerenciar imagens base e instalar software, mas não pode atribuir aplicativos ou desktops a usuários. |
| Administrador de Grupo de Entrega | Pode entregar aplicativos, desktops e máquinas; também pode gerenciar as sessões associadas. Também pode gerenciar configurações de aplicativos e desktops, como políticas e configurações de gerenciamento de energia. |
| Administrador de Host | Pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, aplicativos ou desktops a usuários. |

Em certas edições do produto, você pode criar funções personalizadas para corresponder aos requisitos da sua organização e delegar permissões com mais detalhes. Você pode usar funções personalizadas para alocar permissões na granularidade de uma ação ou tarefa em um console.

- **Escopos:** Um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma que seja relevante para sua organização (por exemplo, o conjunto de Delivery Groups usados pela equipe de Vendas). Os objetos podem estar em mais de um escopo; você pode pensar em objetos sendo rotulados com um ou mais escopos. Existe um escopo integrado: 'Todos', que contém todos os objetos. A função de Administrador Completo está sempre emparelhada com o escopo Todos.

## Exemplo

A Empresa XYZ decidiu gerenciar aplicativos e desktops com base em seu departamento (Contas, Vendas e Armazém) e seu sistema operacional de desktop (Windows 7 ou Windows 8). O administrador criou cinco escopos e, em seguida, rotulou cada Delivery Group com dois escopos: um para o departamento onde são usados e outro para o sistema operacional que utilizam.

Os seguintes administradores foram criados:

| ADMINISTRADOR | FUNÇÕES | ESCOPOS |
|---|---|---|
| domain/fred | Administrador Completo | Todos (a função de Administrador Completo sempre tem o escopo Todos) |
| domain/rob | Administrador Somente Leitura | Todos |
| domain/heidi | Administrador Somente Leitura, Administrador de Suporte Técnico | Todas as Vendas |
| domain/warehouseadmin | Administrador de Help Desk | Armazém |
| domain/peter | Administrador de Grupo de Entrega, Administrador de Catálogo de Máquinas | Win7 |

- Fred é um Administrador Completo e pode visualizar, editar e excluir todos os objetos no sistema.
- Rob pode visualizar todos os objetos no site, mas não pode editá-los ou excluí-los.
- Heidi pode visualizar todos os objetos e realizar tarefas de suporte técnico em Grupos de Entrega no escopo de Vendas. Isso permite que ela gerencie as sessões e máquinas associadas a esses grupos; ela não pode fazer alterações no Grupo de Entrega, como adicionar ou remover máquinas.
- Qualquer pessoa que seja membro do grupo de segurança do Active Directory warehouseadmin pode visualizar e realizar tarefas de suporte técnico em máquinas no escopo de Armazém.
- Peter é um especialista em Windows 7 e pode gerenciar todos os Catálogos de Máquinas do Windows 7 e entregar aplicativos, desktops e máquinas do Windows 7, independentemente do

escopo de departamento em que estejam. A administradora considerou tornar Peter um Administrador Completo para o escopo Win7. No entanto, ela decidiu contra isso, porque um Administrador Completo também tem direitos totais sobre todos os objetos que não estão em escopo, como 'Site' e 'Administrador'.

## Como usar a administração delegada

Geralmente, o número de administradores e a granularidade de suas permissões dependem do tamanho e da complexidade da implantação.

- Em implantações pequenas ou de prova de conceito, um ou poucos administradores fazem tudo. Não há delegação. Neste caso, crie cada administrador com a função de Administrador Completo integrada, que possui o escopo Todos.
- Em implantações maiores com mais máquinas, aplicativos e desktops, é necessária mais delegação. Vários administradores podem ter responsabilidades funcionais (funções) mais específicas. Por exemplo, dois são Administradores Completos e outros são Administradores de Suporte Técnico. Além disso, um administrador pode gerenciar apenas certos grupos de objetos (escopos), como catálogos de máquinas. Neste caso, crie novos escopos, além de administradores com uma das funções integradas e os escopos apropriados.
- Implantações ainda maiores podem exigir mais escopos (ou mais específicos), além de diferentes administradores com funções não convencionais. Neste caso, edite ou crie mais escopos, crie funções personalizadas e crie cada administrador com uma função integrada ou personalizada, além de escopos existentes e novos.

Para flexibilidade e facilidade de configuração, você pode criar escopos ao criar um administrador. Você também pode especificar escopos ao criar ou editar Catálogos de Máquinas ou conexões.

## Criar e gerenciar administradores

Quando você cria um site como administrador local, sua conta de usuário se torna automaticamente um Administrador Completo com permissões totais sobre todos os objetos. Depois que um site é criado, os administradores locais não têm privilégios especiais.

A função de Administrador Completo sempre tem o escopo Todos; você não pode alterar isso.

Por padrão, um administrador é habilitado. Desabilitar um administrador pode ser necessário se você estiver criando o administrador agora, mas essa pessoa não iniciará as tarefas de administração até mais tarde. Para administradores habilitados existentes, você pode querer desabilitar vários deles enquanto reorganiza seus objetos/escopos e, em seguida, reabilitá-los quando estiver pronto para entrar em operação com a configuração atualizada. Você não pode

desabilitar um Administrador Completo se isso resultar na ausência de um Administrador Completo habilitado. A caixa de seleção habilitar/desabilitar está disponível ao criar, copiar ou editar um administrador.

Quando você exclui um par função/escopo ao copiar, editar ou excluir um administrador, ele exclui apenas o relacionamento entre a função e o escopo para esse administrador. Ele não exclui a função nem o escopo. Também não afeta nenhum outro administrador que esteja configurado com esse par função/escopo.

Para criar e gerenciar administradores, siga estas etapas:

1. Faça login no Web Studio, clique em **Administrators** no painel esquerdo e, em seguida, clique na guia **Administrators**.
2. Siga as instruções para a tarefa que deseja concluir:

    - **Criar um administrador:** Clique em **Criar Administrador** na barra de ações. Digite ou procure o nome da conta de usuário, selecione ou crie um escopo e, em seguida, selecione uma função. O novo administrador é habilitado por padrão; você pode alterar isso.
    - **Copiar um administrador:** Selecione o administrador e, em seguida, clique em **Copiar Administrador** na barra de ações. Digite ou procure o nome da conta de usuário. Você pode selecionar e, em seguida, editar ou excluir qualquer um dos pares função/escopo e adicionar novos. O novo administrador é habilitado por padrão; você pode alterar isso.
    - **Editar um administrador:** Selecione o administrador e, em seguida, clique em **Editar Administrador** na barra de ações. Você pode editar ou excluir qualquer um dos pares função/escopo e adicionar novos.
    - **Excluir um administrador:** Selecione o administrador e, em seguida, clique em **Excluir Administrador** na barra de ações. Você não pode excluir um Administrador Completo se isso resultar na ausência de um Administrador Completo habilitado.

O painel superior exibe os administradores que você criou. Selecione um administrador para visualizar seus detalhes no painel inferior. A coluna **Avisos** indica se os pares função e escopo associados ao administrador contêm funções ou escopos inutilizáveis. A seguinte mensagem de aviso aparece se um par função e escopo associado contiver funções ou escopos inutilizáveis:

- Função ou escopo associado não utilizável

> **Importante:**

> Uma mensagem de aviso aparece apenas quando um par função e escopo associado contém funções ou escopos inutilizáveis, ou ambos.

> Para remover o par de função e escopo do administrador, conclua uma das seguintes etapas:

- Exclua o par de função e escopo.
  a. Na barra de ações, clique em **Editar Administrador**.
  b. Na janela **Nome e Detalhes do Administrador**, selecione o par de função e escopo e clique em **Excluir**.
  c. Clique em **Salvar** para sair.
- Exclua o administrador.
  a. Na barra de ações, clique em **Excluir Administrador**.
  b. Na janela de confirmação, clique em **Excluir**.

## Criar e gerenciar funções

Quando os administradores criam ou editam uma função, eles podem habilitar apenas as permissões que eles próprios possuem. Isso impede que os administradores criem uma função com mais permissões do que as que eles têm atualmente e, em seguida, a atribuam a si mesmos (ou editem uma função à qual já estão atribuídos).

Os nomes de função podem conter até 64 caracteres Unicode; eles não podem conter: barra invertida, barra, ponto e vírgula, dois pontos, cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda ou para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo. As descrições podem conter até 256 caracteres Unicode.

Você não pode editar ou excluir uma função interna. Você não pode excluir uma função personalizada se algum administrador a estiver usando.

> **Nota:**

> Apenas certas edições do produto suportam funções personalizadas. Somente as edições que suportam funções personalizadas têm entradas relacionadas na barra de ações.

> Para criar e gerenciar funções, siga estas etapas:

1. Faça login no Web Studio, clique em **Administradores** no painel esquerdo e, em seguida, clique na guia **Funções**.
2. Siga as instruções para a tarefa que você deseja concluir:

   - **Visualizar detalhes da função:** Selecione a função. O painel inferior lista os tipos de objeto e as permissões associadas para a função. Clique na guia **Administrators** no painel inferior para visualizar uma lista de administradores que atualmente têm esta função.
   - **Criar uma função personalizada:** Clique em **Create Role** no painel de ações. Insira um nome e uma descrição. Selecione os tipos de objeto e as permissões.
   - **Copiar uma função:** Selecione a função e, em seguida, clique em **Copy Role** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
   - **Editar uma função personalizada:** Selecione a função e, em seguida, clique em **Edit Role** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
   - **Excluir uma função personalizada:** Selecione a função e, em seguida, clique em **Delete Role** na barra de ações. Quando solicitado, confirme a exclusão.

## Criar e gerenciar escopos

Ao criar um site, o único escopo disponível é o escopo 'Todos', que não pode ser excluído.

Você pode criar escopos usando o procedimento a seguir. Você também pode criar escopos ao criar um administrador; cada administrador deve ser associado a pelo menos um par de função e escopo. Ao criar ou editar desktops, catálogos de máquinas, aplicativos ou hosts, você pode adicioná-los a um escopo existente. Se você não os adicionar a um escopo, eles permanecerão parte do escopo 'Todos'.

A criação de sites não pode ser escopada, nem os objetos de administração delegada (escopos e funções). No entanto, os objetos que você não pode escopar são incluídos no escopo 'Todos'. (Administradores Completos sempre têm o escopo Todos.) Máquinas, ações de energia, desktops e sessões não são diretamente escopados. Os administradores podem receber permissões sobre esses objetos por meio dos catálogos de máquinas ou grupos de entrega associados.

Regras para criar e gerenciar escopos:

- Os nomes de escopo podem conter até 64 caracteres Unicode. Os nomes de escopo não podem incluir: barra invertida, barra, ponto e vírgula, dois pontos, sinal de cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda, seta para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo.
- As descrições de escopo podem conter até 256 caracteres Unicode.
- Ao copiar ou editar um escopo, lembre-se de que a remoção de objetos do escopo pode tornar esses objetos inacessíveis ao administrador. Se o escopo editado estiver emparelhado com uma ou mais funções, certifique-se de que as atualizações do escopo não tornem nenhum par função/escopo inutilizável.

Para criar e gerenciar escopos, siga estas etapas:

1. Faça login no Web Studio, clique em **Administrators** no painel esquerdo e, em seguida, clique na guia **Scopes**.
2. Siga as instruções para a tarefa que você deseja concluir:

    - **Criar um escopo:** Clique em **Criar novo escopo** na barra de ações. Insira um nome e uma descrição. Para incluir todos os objetos de um tipo específico (por exemplo, Grupos de Entrega), selecione o tipo de objeto. Para incluir objetos específicos, expanda o tipo e selecione objetos individuais (por exemplo, Grupos de Entrega usados pela equipe de Vendas).
    - **Copiar um escopo:** Selecione o escopo e clique em **Copiar escopo** na barra de ações. Insira um nome e uma descrição. Altere os tipos de objeto e os objetos, conforme necessário.
    - **Editar um escopo:** Selecione o escopo e clique em **Editar escopo** na barra de ações. Altere o nome, a descrição, os tipos de objeto e os objetos, conforme necessário.
    - **Excluir um escopo:** Selecione o escopo e clique em **Excluir escopo** na barra de ações. Quando solicitado, confirme a exclusão.

## Criar relatórios

Você pode criar dois tipos de relatórios de administração delegada:

- Um relatório HTML que lista os pares função/escopo associados a um administrador, além das permissões individuais para cada tipo de objeto (por exemplo, grupos de entrega e catálogos de máquinas). Você gera este relatório a partir do Web Studio.

  Para criar este relatório, siga estas etapas:

a. Faça login no Web Studio, clique em **Administradores** no painel esquerdo

b. Selecione um administrador e clique em **Criar Relatório** na barra de ações.

Você também pode solicitar este relatório ao criar, copiar ou editar um administrador.

- Um relatório HTML ou CSV que mapeia todas as funções internas e personalizadas para permissões. Você gera este relatório executando um script PowerShell chamado OutputPermissionMapping.ps1.

  Para executar este script, você deve ser um Administrador Completo, um Administrador Somente Leitura ou um administrador personalizado com permissão para ler funções. O script está localizado em: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

  Sintaxe:

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

| PARÂMETRO | DESCRIÇÃO |
|---|---|
| `-Help` | Exibe a ajuda do script. |
| `-Csv` | Especifica a saída CSV. Padrão = HTML |
| `-Path string` | Onde gravar a saída. Padrão = stdout |
| `-AdminAddress string` | Endereço IP ou nome do host do Delivery Controller™ ao qual se conectar. Padrão = localhost |
| `-Show` | (Válido apenas quando o parâmetro `-Path` também é especificado) Ao gravar a saída em um arquivo, `-Show` faz com que a saída seja aberta em um programa apropriado, como um navegador da web. |
| Parâmetros Comuns | `Verbose`, `Debug`, `ErrorAction`, `ErrorVariable`, `WarningAction`, `WarningVariable`, `OutBuffer` e `OutVariable`. Para obter detalhes, consulte a documentação da Microsoft. |

O exemplo a seguir grava uma tabela HTML em um arquivo chamado Roles.html e abre a tabela em um navegador da web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

O exemplo a seguir grava uma tabela CSV em um arquivo chamado Roles.csv. A tabela não é exibida.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

A partir de um prompt de comando do Windows, o comando de exemplo anterior é:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

# Controladores de Entrega

**Nota:**

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

> O Delivery Controller é o componente do lado do servidor responsável por gerenciar o acesso do usuário, além de intermediar e otimizar conexões. Os Controladores também fornecem os Machine Creation Services™ que criam imagens de desktop e servidor.

Um site deve ter pelo menos um Controlador. Após instalar o Controlador inicial, você pode adicionar mais Controladores ao criar um site, ou posteriormente. Existem dois benefícios principais em ter mais de um Controlador em um site.

- **Redundância:** Como melhor prática, em um site de produção, sempre tenha pelo menos dois Controladores em servidores físicos diferentes. Se um Controlador falhar, os outros podem gerenciar as conexões e administrar o site.
- **Escalabilidade:** À medida que a atividade do site aumenta, o mesmo acontece com a utilização da CPU no Controlador e a atividade do banco de dados. Controladores adicionais permitem que você manipular mais usuários e mais solicitações de aplicativos e desktops, e podem melhorar a capacidade de resposta geral.

Cada Controlador se comunica diretamente com o banco de dados do site. Em um site com mais de uma zona, os Controladores em cada zona se comunicam com o banco de dados do site na zona primária.

> **Importante:**

> Não altere o nome do computador ou a associação ao domínio de um Controlador após a configuração do site.

## Como os VDAs se registram nos Controladores

Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) com um Delivery Controller no site. Para obter informações sobre o registro de VDA, consulte Registro de VDA com Controladores.

## Adicionar, remover ou mover Controladores

Para adicionar, remover ou mover um Controlador, você deve ter as permissões de função de servidor e função de banco de dados listadas no artigo Bancos de Dados.

Não há suporte para a instalação de um Controlador em um nó em uma instalação de cluster SQL ou espelhamento SQL.

Ao adicionar um Delivery Controller™ a um site, certifique-se de adicionar as credenciais de logon para essa máquina a quaisquer SQL Servers de réplica que você usa para alta disponibilidade.

Se sua implantação usa espelhamento de banco de dados:

- Antes de adicionar, remover ou mover um Controller, certifique-se de que os bancos de dados principal e espelhado estejam ambos em execução. Além disso, se você estiver usando scripts com o SQL Server Management Studio, habilite o modo SQLCMD antes de executar os scripts.
- Para verificar o espelhamento após adicionar, remover ou mover um Controller, execute o cmdlet PowerShell `Get-configdbconnection`. Esse cmdlet garante que o Failover Partner tenha sido definido na string de conexão para o espelho.

Depois de adicionar, remover ou mover um Controller:

- Se a atualização automática estiver ativada, os VDAs recebem uma lista atualizada de Controllers em até 90 minutos.
- Se a atualização automática não estiver ativada, certifique-se de que a configuração da política do Controller ou a chave de registro ListOfDDCs sejam atualizadas para todos os VDAs. Depois de mover um Controller para outro site, atualize a configuração da política ou a chave de registro em ambos os sites.

### Adicionar um Controller

Você pode adicionar Controllers ao criar um site e posteriormente. Não é possível adicionar Controllers instalados com uma versão anterior deste software a um site que foi criado com esta versão.

1. Execute o instalador em um servidor que contenha um sistema operacional compatível. Instale o componente Delivery Controller e quaisquer outros componentes principais que desejar. Conclua o assistente de instalação.
2. Se você ainda não criou um site, execute Citrix Site Manager neste Controller para criar um site. O endereço IP deste Controller é adicionado automaticamente ao novo site.

   Se você planeja gerar scripts que inicializam os bancos de dados, adicione os Controllers antes de gerar os scripts.
3. Se você já criou um site, siga estas etapas:

   a. Execute Citrix Site Manager neste Controller, clique em **Ingressar em um site existente** e digite o endereço de um Controller no site ao qual você deseja ingressar.

b. Execute ferramenta de configuração do Studio para adicionar o Controller ao Web Studio.

### Remover um Controller

Remover um Controller de um site não desinstala o software Citrix ou qualquer outro componente. Essa ação remove o Controller do banco de dados para que ele não possa mais ser usado para intermediar conexões e executar outras tarefas. Se você remover um Controller, poderá adicioná-lo novamente ao mesmo site ou a outro site. Um site requer pelo menos um Controller, portanto, você não pode remover o último listado no Web Studio.

Quando você remove um Controller de um site, o logon do Controller para o servidor de banco de dados não é removido. Isso evita a remoção potencial de um logon que é usado por serviços de outros produtos na mesma máquina. O logon deve ser removido manualmente se não for mais necessário. A permissão de função de servidor `securityadmin` é necessária para remover o logon.

Depois de remover um Controller:

- Os VDAs que usam a atualização automática se registram novamente com outros Controllers disponíveis. Esse novo registro ocorre somente se o mecanismo de atualização automática estiver habilitado e os VDAs puderem alcançar outros controllers (na mesma zona secundária que o Controller removido ou na zona primária para implantações locais).
- Atualize as informações do Controller no Citrix StoreFront. Para obter mais informações, consulte Gerenciar Controllers.
- No Citrix StoreFront, atualize os URLs da Secure Ticket Authority (STA) para acesso remoto através do Citrix Gateway. Para obter mais informações, consulte Gerenciar Secure Ticket Authorities.
- No Citrix Gateway, atualize quaisquer URLs STA do servidor virtual. Para obter mais informações, consulte Citrix Gateway.

> **Importante:**
>
> Não remova o Controller do Active Directory antes de removê-lo do site.

1. Certifique-se de que o Controller esteja ligado para que o Web Studio possa carregar e exibir o Controller que você deseja remover.
2. Depois que o Web Studio carregar completamente o Controller, verifique se todos os serviços no Controller estão em execução e se o Controller permanece ligado.

3. Faça login no Web Studio, selecione **Configurações** no painel esquerdo.
4. Localize o bloco **Delivery Controller** e clique em **Editar**.
5. Na página **Gerenciar Delivery Controller**, selecione o Controller que você deseja remover.
6. Selecione **Remover Controller**. Se você não tiver as funções e permissões de banco de dados corretas, será oferecida a opção de gerar um script que permite ao seu administrador de banco de dados remover o Controller para você.

   O Web Studio executa uma verificação prévia antes de remover um Controller. Um controller é seguro para remover se estiver desligado e não estiver no seguinte status de serviço:

   - Desconhecido
   - Falha pendente
   - Versão mais antiga
   - Versão mais recente
   - Alteração de versão em andamento
   - Recursos obrigatórios ausentes

   Se o Controller não estiver desligado e estiver em qualquer um dos status de serviço mencionados, o Web Studio solicitará que você desligue o Controller.
7. Você deve remover a conta de máquina do Controller do servidor de banco de dados. Antes de remover, verifique se outro serviço não está usando a conta.

Depois de usar o Web Studio para remover um Controller, o tráfego para esse Controller pode persistir por um curto período de tempo para garantir a conclusão adequada das tarefas atuais. Se você quiser forçar a remoção de um Controller em um curto espaço de tempo, a Citrix recomenda que você desligue o servidor onde ele foi instalado ou remova esse servidor do Active Directory. Em seguida, reinicie os outros Controllers no site para garantir que não haja mais comunicação com o Controller removido.

### Mover um Controller para outra zona

Se o seu site contiver mais de uma zona, você poderá mover um Controller para uma zona diferente. Consulte as Zonas para obter informações sobre como essa movimentação pode afetar o registro de VDA e outras operações.

1. Selecione **Zona** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione um Controller.
3. Selecione **Mover Itens** na barra de ações.

4. Na página **Mover Itens** que aparece, selecione a zona para onde você deseja mover o Controller.
5. Clique em **Salvar**.

## Mover um VDA para outro site

Se um VDA foi provisionado usando Citrix Provisioning™ ou é uma imagem existente, você pode mover um VDA para outro site (do site 1 para o site 2) ao atualizar, ou ao mover uma imagem de VDA que foi criada em um site de teste para um site de produção. VDAs provisionados usando Machine Creation Services (MCS) não podem ser movidos de um site para outro. O MCS não oferece suporte à alteração do ListOfDDCs que um VDA verifica para se registrar em um Controller. VDAs provisionados usando MCS sempre verificam o ListOfDDCs associado ao site em que foram criados.

Existem duas maneiras de mover um VDA para outro site: usando o instalador ou as políticas do Citrix.

### Instalador

Execute o instalador e adicione um Controller, especificando o FQDN (entrada DNS) de um Controller no site 2.

Especifique os Controllers no instalador somente quando a configuração da política de Controllers não for usada.

### Editor de Política de Grupo

O exemplo a seguir move vários VDAs entre sites.

1. Crie uma política no site 1 que contenha as seguintes configurações e, em seguida, filtre a política para o nível do Grupo de Entrega para iniciar uma migração de VDA em etapas entre os sites.
    - Controllers: Contendo FQDNs (entradas DNS) de um ou mais Controllers no site 2.
    - Habilitar atualização automática de Controllers: definido como desabilitado.
2. Cada VDA no Grupo de Entrega é alertado em até 90 minutos sobre a nova política. O VDA ignora a lista de Controllers que recebe (porque a atualização automática está desabilitada); ele seleciona um dos Controllers especificados na política, que lista os Controllers no site 2.
3. Quando o VDA se registra com sucesso em um Controller no site 2, ele recebe a ListOfDDCs do site 2 e as informações da política, que têm a atualização automática habilitada por padrão. O Controller com o qual o VDA foi registrado no site 1 não está na lista enviada pelo Controller

no site 2. Assim, o VDA se registra novamente, escolhendo entre os Controllers na lista do site 2. A partir de então, o VDA é atualizado automaticamente com informações do site 2.

Para obter informações sobre como usar o Editor de Política de Grupo, consulte a documentação Citrix policies.

## Suporte a IPv4/IPv6

Esta versão oferece suporte a implantações puras de IPv4, puras de IPv6 e de pilha dupla que usam redes IPv4 e IPv6 sobrepostas.

Os seguintes componentes suportam apenas IPv4. Todos os outros suportam IPv4 e IPv6.

- XenServer®
- Virtual Delivery Agents (VDAs) não controlados pela configuração de política **Only use IPv6 Controller registration**

As comunicações IPv6 são controladas com duas configurações de política Citrix® relacionadas à conexão VDA.

- **Configuração principal que impõe o uso de IPv6:** Only use IPv6 Controller registration.

  Essa configuração de política controla qual forma de endereço o VDA usa para se registrar no Delivery Controller.

  Quando ativado, o VDA se registra e se comunica com o Controller usando um único endereço IPv6 escolhido na seguinte precedência: endereço IP global, Unique Local Address (ULA), endereço link-local (somente se nenhum outro endereço IPv6 estiver disponível).

  Quando desativado, o VDA se registra e se comunica com o Controller usando o endereço IPv4 da máquina. Este é o valor padrão.

  Se uma equipe usa frequentemente uma rede IPv6, publique os desktops e aplicativos para esses usuários com base em uma imagem ou Unidade Organizacional (OU) que tenha a configuração de política **Only use IPv6 Controller registration** ativada.

  Se uma equipe usa frequentemente uma rede IPv4, publique os desktops e aplicativos para esses usuários com base em uma imagem ou OU que tenha a configuração de política **Only use IPv6 Controller registration** desativada.
- **Configuração dependente que define uma máscara de rede IPv6:** Controller registration IPv6 netmask.

Uma máquina pode ter vários endereços IPv6. Essa configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial, em vez de um IP global, se um estiver registrado. Essa configuração especifica a rede onde o VDA se registra. O VDA se registra apenas no primeiro endereço que corresponde à máscara de rede especificada.

Essa configuração é válida apenas quando a configuração de política **Only use IPv6 Controller registration policy** está ativada. Padrão = String vazia

### Considerações de implantação

Se seu ambiente contiver redes IPv4 e IPv6, crie configurações de grupo de entrega separadas para clientes somente IPv4 e para clientes que podem acessar a rede IPv6. Considere usar nomes, atribuição manual de grupo do Active Directory ou filtros SmartAccess para diferenciar os usuários. A reconexão da sessão pode falhar se a conexão começar em uma rede IPv6 e você tentar se conectar novamente de um cliente que tem apenas acesso IPv4.

NOTA - Essas considerações não se aplicam se você tiver resolução de DNS habilitada

## Licenciamento para Citrix Virtual Apps and Desktops™ usando o Web Studio

**Observação:**

- Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.
- O Serviço de Ativação de Licenças (LAS) é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa ao licenciamento legado tradicional da Citrix®. O LAS introduz novos módulos para ativação, garantindo uma abordagem moderna e contínua para o gerenciamento de licenças. Consulte Serviço de Ativação de Licenças para obter mais informações.

No Web Studio, você pode gerenciar e rastrear o licenciamento, se o servidor de licenças estiver no mesmo domínio do Web Studio ou em um domínio confiável. Para obter informações sobre tarefas de licenciamento, consulte a documentação de licenciamento e Licenciamento de vários tipos.

A tabela a seguir lista as edições e os modelos de licença compatíveis:

| PRODUTOS | EDIÇÕES | MODELOS DE LICENÇA |
|---|---|---|
| Citrix Virtual Apps | Premium, Advanced, Standard | Concorrente |
| Citrix Virtual Desktops | Premium, Advanced, Standard | Usuário/Dispositivo e Concorrente |

Para obter mais informações, consulte Licença Concorrente e Licença de Usuário/Dispositivo.

## Versão de Current Release (CRs) e Long Term Service Release (LTSRs) suportadas

A tabela a seguir lista a **versão mínima compatível do LS** para Citrix Virtual Apps and Desktops, XenApp e XenDesktop. Para obter mais informações sobre as datas de ciclo de vida dos produtos Citrix, consulte Matriz de Produtos.

**Importante:**

As informações na tabela a seguir são fornecidas apenas para compatibilidade de produtos. A Citrix recomenda fortemente que você sempre use a versão mais recente disponível do Citrix License Server para se beneficiar de quaisquer melhorias funcionais ou de segurança que ela possa conter.

**Observação:**

O License Server VPX foi descontinuado e não receberá mais manutenção ou correções de segurança. Os clientes que usam a versão 11.16.6 ou versões anteriores do License Server VPX são aconselhados a migrar para a versão mais recente do License Server para Windows o mais rápido possível.

| VERSÃO ATUAL | VERSÃO MÍNIMA COMPATÍVEL DO LS |
|---|---|
| 2305 | 11.17.2.0 Build 35000 |
| 2303 | 11.17.2.0 Build 35000 |
| 2212 | 11.17.2.0 Build 35000 |
| 2209 | 11.17.2.0 Build 35000 |
| 2206 | 11.17.2.0 Build 35000 |
| 2203 | 11.17.2.0 Build 35000 |
| 2112 | 11.17.2.0 Build 35000 |
| 2109 | 11.17.2.0 Build 35000 |
| 2106 | 11.17.2.0 Build 35000 |
| 2103 | 11.16.3.0 Build 28000 |

| VERSÃO DE SERVIÇO DE LONGO PRAZO | VERSÃO MÍNIMA COMPATÍVEL DO LS |
|---|---|
| 2203 LTSR | 11.17.2.0 Build 35000 |
| 1912 LTSR | 11.16.3.0 Build 28000 |
| 7.15 LTSR | 11.15.0.0 Build 24100 |
| 7.6 LTSR | 11.14.0.1 Build 21103 |

Para obter informações sobre produtos legados e versões de produtos, consulte a Matriz de Produtos Legados.

Você deve ser um administrador de licenças completo para concluir as seguintes tarefas. Para visualizar informações de licença no Web Studio, um administrador deve ter pelo menos a permissão de administração delegada de Leitura de Licenciamento. As funções internas de Administrador Completo e Administrador Somente Leitura possuem essa permissão.

## Baixar e instalar uma licença da Citrix usando o Web Studio

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Alocar Licenças** na barra de ações.
3. Insira o Código de Acesso da Licença, que você recebeu em um e-mail da Citrix após a compra ou renovação das licenças.
4. Selecione um produto e escolha **Alocar Licenças**. As licenças disponíveis para esse produto são alocadas e baixadas. Depois de alocar e baixar todas as licenças para um Código de Acesso da Licença específico, você não poderá reutilizar esse Código de Acesso da Licença. Para realizar outras transações com o mesmo código, faça login em Minha Conta.

## Adicionar licenças armazenadas no seu computador local ou na rede

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Adicionar Licenças** na barra de ações.
3. Procure um arquivo de licença e adicione-o ao servidor de licenças.

## Alterar o servidor de licenças

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Alterar Servidor de Licenças** na barra de ações.
3. Digite o endereço do servidor de licenças no formato *nome:porta*, onde o nome é um DNS, NetBIOS ou endereço IP. Se você não especificar um número de porta, a porta padrão (27000) será usada.

## Selecione o tipo de licença a ser usado

- Ao configurar o Site, depois de especificar o servidor de licenças, você será solicitado a selecionar o tipo de licença a ser usado. Se não houver licenças no servidor, a opção de usar o produto por um período de avaliação de 30 dias sem licença será selecionada automaticamente.
- Se houver licenças no servidor, seus detalhes serão exibidos e você poderá selecionar uma delas. Ou, você pode adicionar um arquivo de licença ao servidor e então selecionar esse.

## Alterar a edição do produto e o modelo de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Editar Edição do Produto** na barra de ações.

3. Atualize as opções apropriadas.

Para acessar o Console de Administração de Licenças, na barra de ações, selecione **Console de Administração de Licenças**. O console aparece imediatamente ou, se o painel estiver configurado com proteção por senha, você será solicitado a fornecer as credenciais do Console de Administração de Licenças. Para obter detalhes sobre como usar o console, consulte a documentação de licenciamento.

> **Observação:**
>
> Ao alternar licenças no Web Studio, a alteração leva até 5 minutos para aparecer no Citrix Director. Por exemplo, se você alternar entre Advanced e Premium ou vice-versa.

## Adicionar um administrador de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento**.
3. Selecione **Adicionar administrador de licenciamento** na barra de ações.
4. Navegue até o usuário que você deseja adicionar como administrador e escolha as permissões.

## Alterar as permissões de um administrador de licenciamento ou excluir um administrador de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento** e, em seguida, selecione o administrador.
3. Selecione **Editar administrador de licenciamento** ou **Excluir administrador de licenciamento** na barra de ações.

## Adicionar um grupo de administradores de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento**.
3. Selecione **Adicionar grupo de administradores de licenciamento** na barra de ações.

4. Navegue até o grupo que você deseja que atue como administradores de licenciamento e escolha as permissões. Adicionar um Grupo do Active Directory concede permissões de administrador de licenciamento aos usuários dentro desse grupo.

## Alterar as permissões de um grupo de administradores de licenciamento ou excluir um grupo de administradores de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento** e, em seguida, selecione o grupo de administradores.
3. Selecione **Editar grupo de administradores de licenciamento** ou **Excluir grupo de administradores de licenciamento** na barra de ações.

## Exibir informações da licença

Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo. Um resumo do uso da licença e das configurações do Site é exibido com uma lista de todas as licenças atualmente instaladas no servidor de licenças especificado.

Certifique-se de que as configurações de licenciamento do site, que incluem o tipo de produto, a edição da licença e o modelo de licenciamento, correspondam às licenças que seu Servidor de Licenças configurado usa. Caso contrário, talvez seja necessário baixar ou alocar suas licenças existentes para corresponder às configurações de licença do site.

## Exibir alertas de expiração de licença

O Web Studio consulta as datas de expiração dos arquivos de licença no Citrix License Server. O Web Studio alerta os administradores na guia Visão Geral se os arquivos de licença estiverem próximos da expiração ou já tiverem expirado.

## Ofuscar dados de telemetria de licenciamento

Considerando a sensibilidade das informações enviadas na telemetria de licença, a Citrix oferece uma opção para ofuscar os dados.

A tabela a seguir lista os dados que podem ser ofuscados:

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| usuário | Identifica o ID do Usuário para identificar de forma | - nomeCompleto: `C648FE671A44B3F7` |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| | exclusiva um usuário que inicia o lançamento da sessão. | |
| | - nomeSam: `C758LH671A44B3F7` | |
| | - UPN: `C7948FE671A44B3F7` | |
| | - idLicencaUsuario: `C265FE671A44B3F7` | |
| | - userSid: `C097FE671A44B3F7` | |
| dvc para dvcName | Indica o nome amigável para o dispositivo. | `C758LH671A44B3F7` |
| workerSid | Indica um identificador exclusivo para o VDA usado para a sessão. | `1E5LH671A44B3F7` |
| AdminLoginList | Indica a lista de SamAccountName de administradores exclusivos | `{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw==]}` |

Para habilitar ou desabilitar a ofuscação, execute os seguintes comandos PowerShell no Delivery Controller.

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando para habilitar ou desabilitar a ofuscação:

   Por padrão, o valor é `1`, ou `true`, o que habilita a ofuscação dos dados de telemetria de licença.

   Para desabilitar:

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $false
```

Depois de desabilitar a ofuscação, você pode habilitá-la usando o seguinte comando:

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

## Links relacionados

- Consulte Assinatura local da Citrix para licenças de varejo anuais e baseadas em prazo.
- Consulte Transição e Upgrade (TTU) com Direitos Híbridos.

## Serviço de Ativação de Licenças

O Serviço de Ativação de Licenças (LAS) é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa ao licenciamento legado tradicional da Citrix®. O LAS introduz novos módulos para ativação, garantindo uma abordagem moderna e contínua para o gerenciamento de licenças.

O LAS simplifica a experiência de licenciamento da Citrix. Não há mais códigos de acesso ou arquivos de licença para gerar, baixar ou instalar no License Server. Você só precisa atualizar seu License Server e registrar-se no Citrix Cloud. Uma vez que os produtos compatíveis são apontados para o License Server, eles podem ser ativados automaticamente.

Após a ativação, o License Server se comunica regularmente com o Serviço de Ativação de Licenças para manter sua ativação atualizada. O LAS é construído com tecnologia de nuvem, o que melhora o desempenho e garante que não haja tempo de inatividade. Se, por qualquer motivo, o License Server ou o LAS estiver inacessível, o sistema entra no modo de cache de licenças, que foi projetado para proteger o sistema de ficar sem licença e evitar uma interrupção. Para obter mais informações, consulte Modo de cache de licenças.

Para mais detalhes sobre o LAS, consulte a documentação de Licenciamento Serviço de Ativação de Licenças.

### Pré-requisitos

- Instale ou atualize o License Server para a versão 11.17.2 build 53100 ou posterior.
- Conexão de internet confiável e contínua para o License Server.

- As configurações de licença no nível do Grupo de Desktops devem ser desabilitadas.

> **Observação:**
>
> Para garantir que o licenciamento no nível DG esteja desabilitado, use Get-brokerdesktopgroup  e LicenseModel deve ser "None".

### Considerações

- Todos os Delivery Controllers devem ser compatíveis com o LAS antes que o Citrix Studio ou o Citrix Web Studio solicitem a ativação. Um site de controlador único pode usar licenças legadas ou LAS.
- Você pode ter vários License Servers registrados com o mesmo Citrix Cloud ID (CCID) ou OrgID. No entanto, um site pode ser configurado para apontar para apenas um License Server.

### Limitações

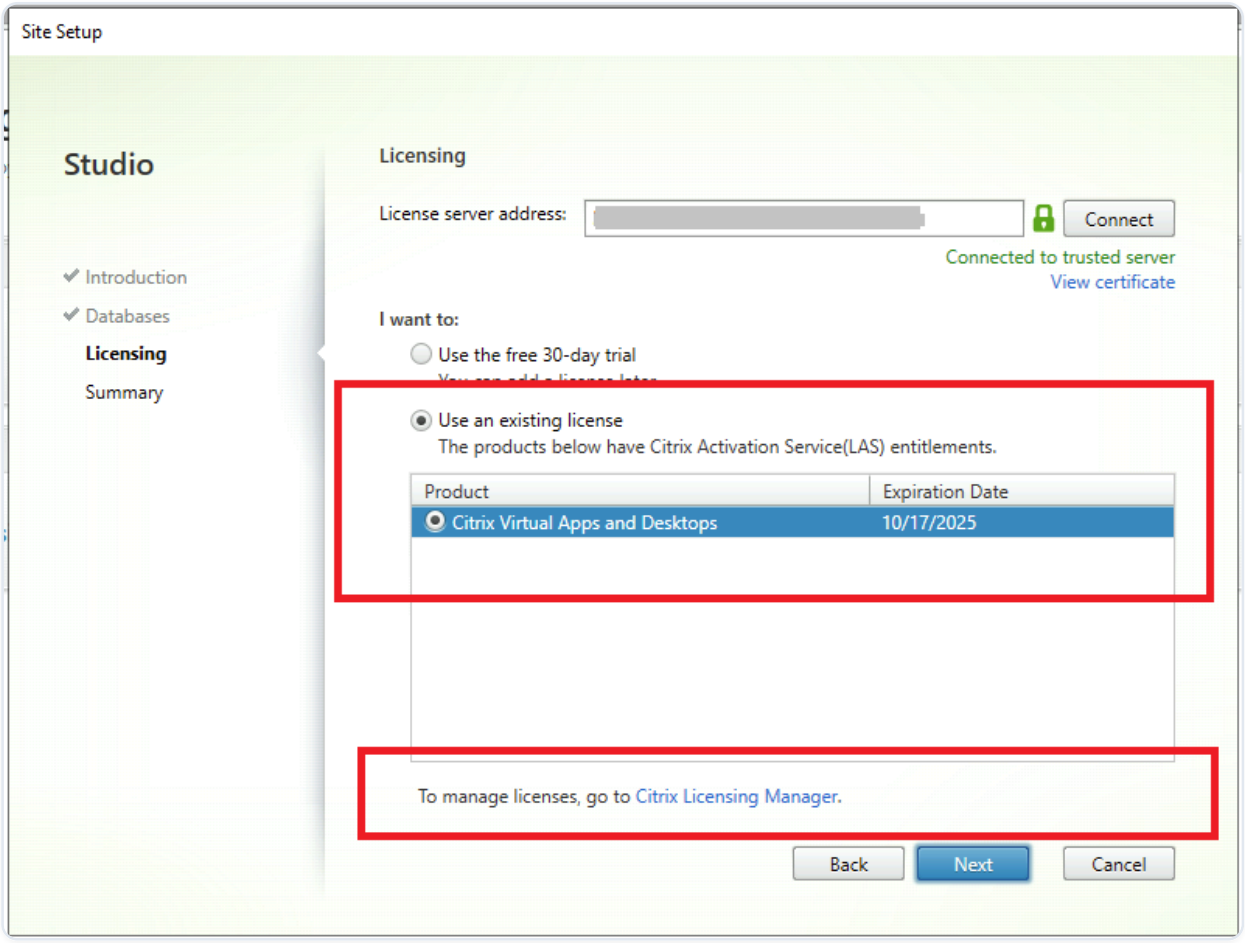
- Migrar para LAS define a Edição do Produto como **Premium** e o Modelo de Licença como **Concorrente**, mas isso pode mudar no futuro. Não modifique a configuração da licença usando o PowerShell, pois isso pode afetar o registro e o início da sessão.
- Você pode migrar seu site Citrix Virtual Apps and Desktops™ da licença legada existente para o LAS usando apenas o Web Studio.

### Etapas principais

1. Instale ou atualize o License Server para a versão 11.17.2 build 53100 ou posterior e configure o LAS conforme as instruções mencionadas em Como configurar o License Server para o Serviço de Ativação de Licenças.
2. Instale o Citrix Virtual Apps and Desktops versão 2402 LTSR CU3 ou posterior. Instale os componentes principais, como Citrix Delivery Controller, Citrix Studio, Web Studio e Citrix Director.

   > **Observação:**
   >
   > Todos os Delivery Controllers no site do Citrix Virtual Apps and Desktops devem ser compatíveis com o LAS.

3. Após instalar os componentes necessários, use o Citrix Site Manager para criar um site. Para obter informações sobre como criar um site, consulte Criar um site. Se o License Server estiver configurado para usar o LAS, o Metainstaller exibirá os direitos. Os direitos são fornecidos juntamente com suas respectivas datas de expiração da licença.




**Observação:**

Se o License Server não for atualizado para a versão 53100 ou posterior, você encontrará erros de licenciamento. Ignorar esses erros e prosseguir com a atualização do site CVAD resultará na inoperabilidade do site.

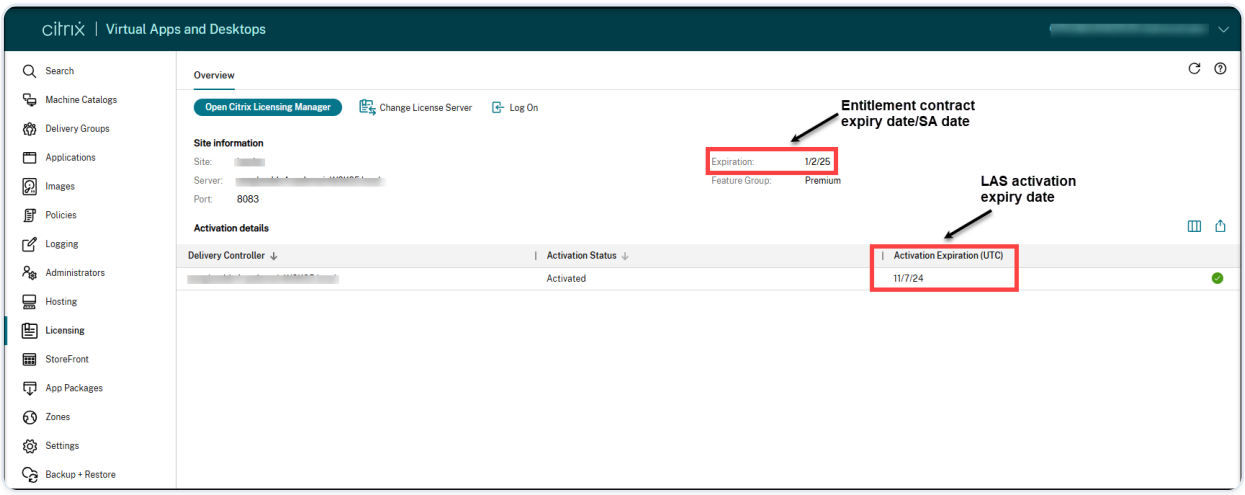
4. Verificar detalhes de licenciamento.
5. Migrar licenciamento herdado para LAS.

### Verificar detalhes de licenciamento

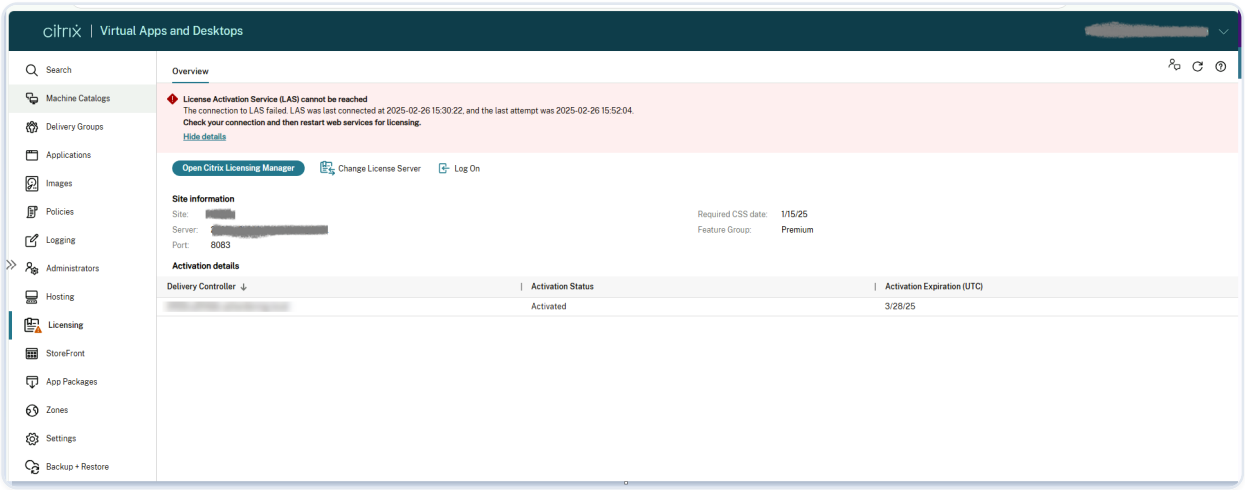
Após criar o site, verifique os detalhes de licenciamento usando o Web Studio.

1. No Web Studio, selecione o nó **Licenciamento**.

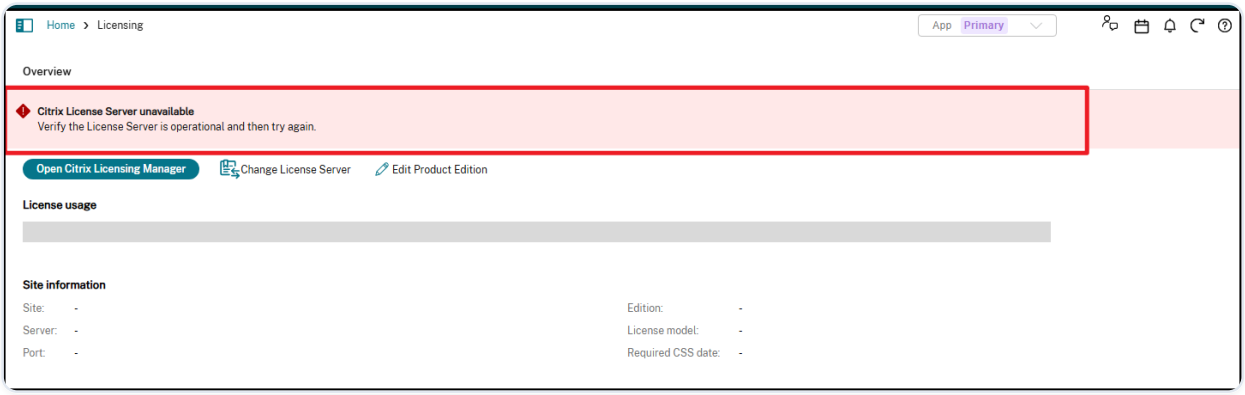
2. Na guia **Visão geral**, verifique se o site do Citrix Virtual Apps and Desktops tem a licença apropriada ou se a licença expirou enquanto usava os recursos do LAS.



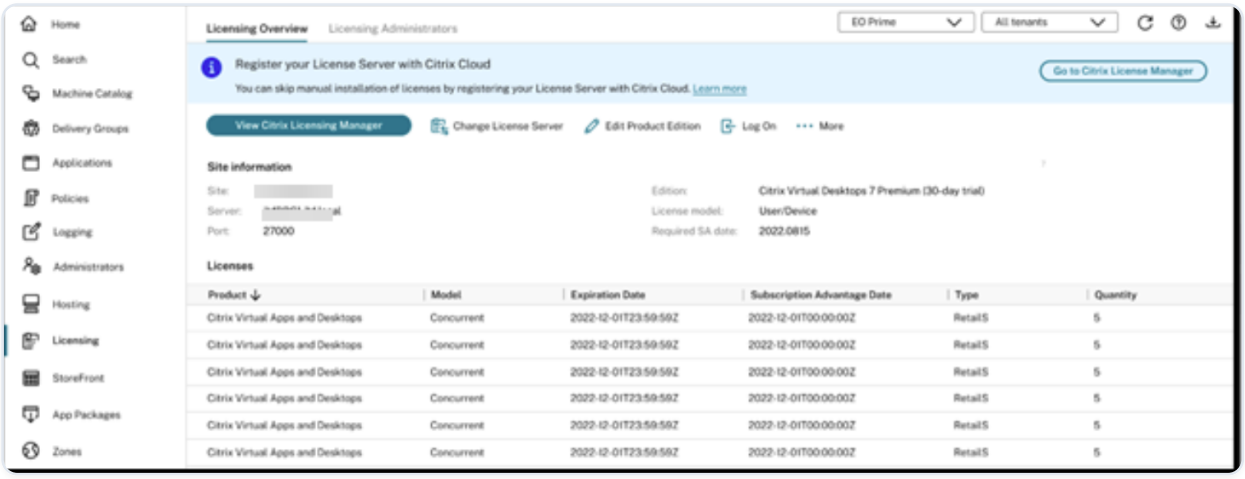

Se o LAS não estiver acessível, você poderá ver uma mensagem de erro:




Se o License Server não estiver disponível, você poderá ver uma mensagem de erro:



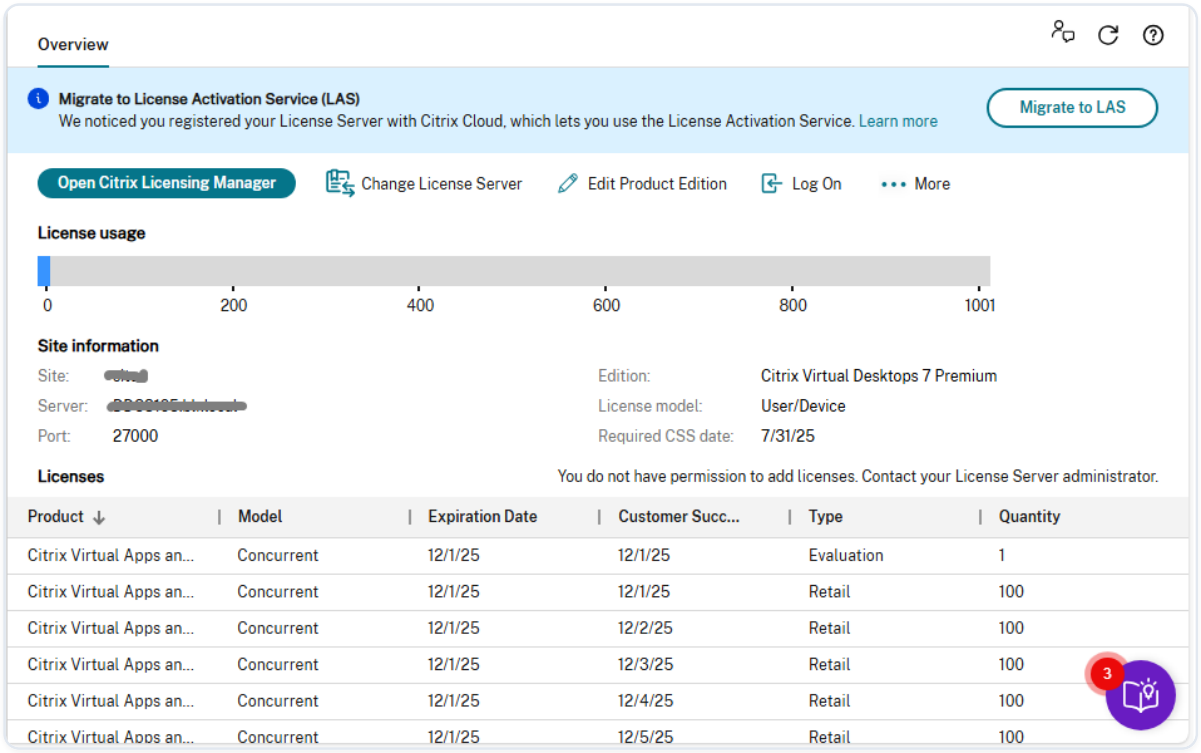

Se o seu Servidor de Licenças ainda estiver usando uma licença herdada antiga e o site do Citrix Virtual Apps and Desktops for compatível com LAS, o Web Studio solicitará que você registre seu Servidor de Licenças no Citrix Cloud.




## Migrar licenciamento herdado para LAS

Se você já registrou seu Servidor de Licenças no Citrix Cloud e tem o direito necessário, deve seguir a sequência específica abaixo para migrar seu site existente do Citrix Virtual Apps and Desktops do licenciamento herdado para o LAS sem impactar as sessões do usuário.

1. **Atualizar Servidor de Licenças:** Atualize o Servidor de Licenças para a versão mínima suportada.
2. **Atualizar Delivery Controllers:** Atualize todos os Delivery Controllers no site para uma versão compatível com LAS.
3. **Remover Atribuições de Licença do Grupo de Entrega:**
    - Antes de clicar em **Migrar para LAS**, remova manualmente quaisquer atribuições de licença definidas abaixo do nível do Site (ou seja, remova a atribuição de licença no nível do grupo de entrega).
4. **Confirmar Alocações:** Verifique se as alocações LAS estão precisas.
5. **Clique em Migrar para LAS:**
    - Assim que as etapas anteriores estiverem concluídas, clique em **Migrar para LAS**.




- A **Edição da Licença** do site do Citrix Virtual Apps and Desktops é definida como **Citrix Virtual Apps and Desktops Premium** e o **Modelo de Licença** é configurado como **Concorrente** assim que você migra para o LAS.

### Reverter de LAS para licenciamento legado

Faça o seguinte para reverter de LAS para licenciamento legado:

1. Execute o seguinte comando PowerShell.

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. Configure as licenças legadas no Web Studio.

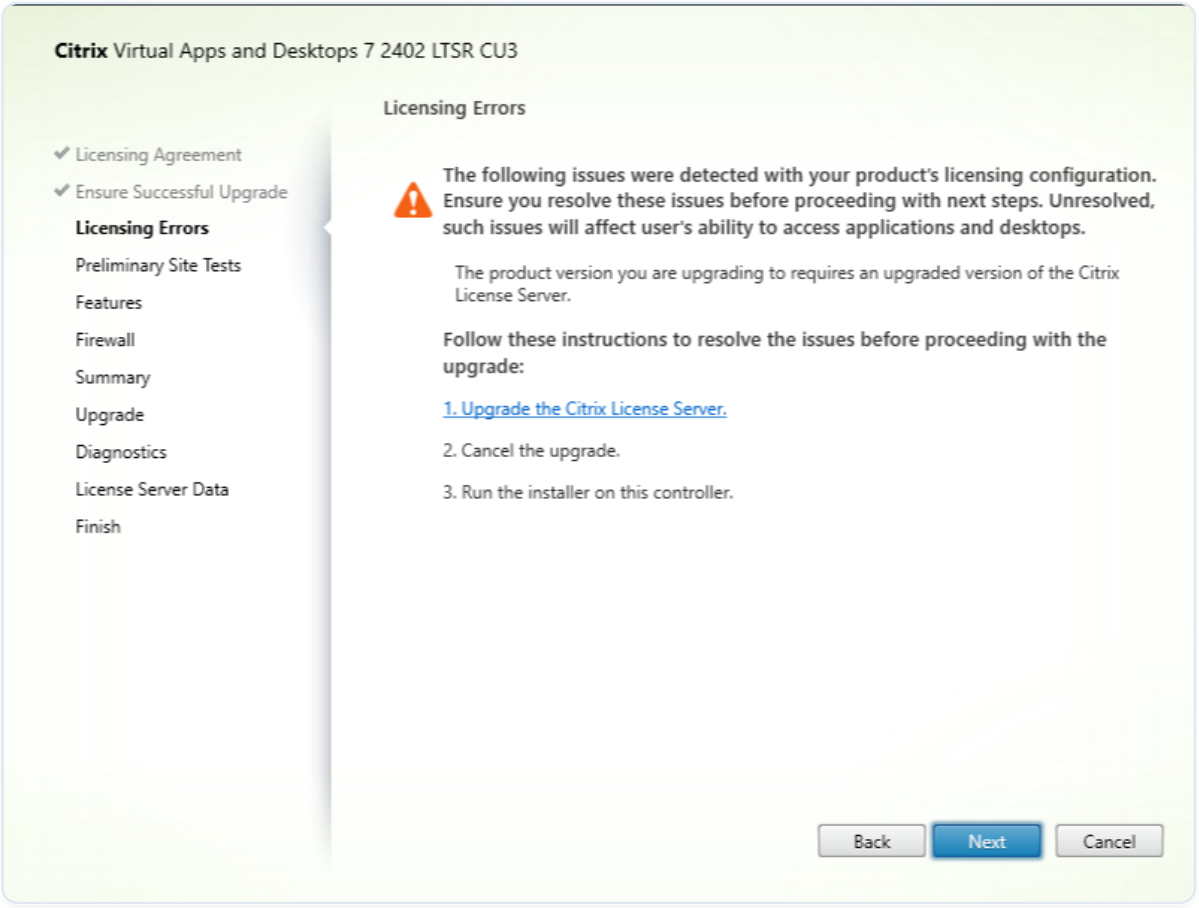
**Observação:**

Estas etapas são fornecidas apenas para solução de problemas temporária. Os arquivos de licença legados estão se aproximando do Fim da Vida Útil (EOL) e não funcionarão após April 15, 2026. Para garantir um serviço ininterrupto, recomendamos a migração para o Serviço de Ativação de Licenças (LAS). Para obter detalhes, consulte o anúncio.

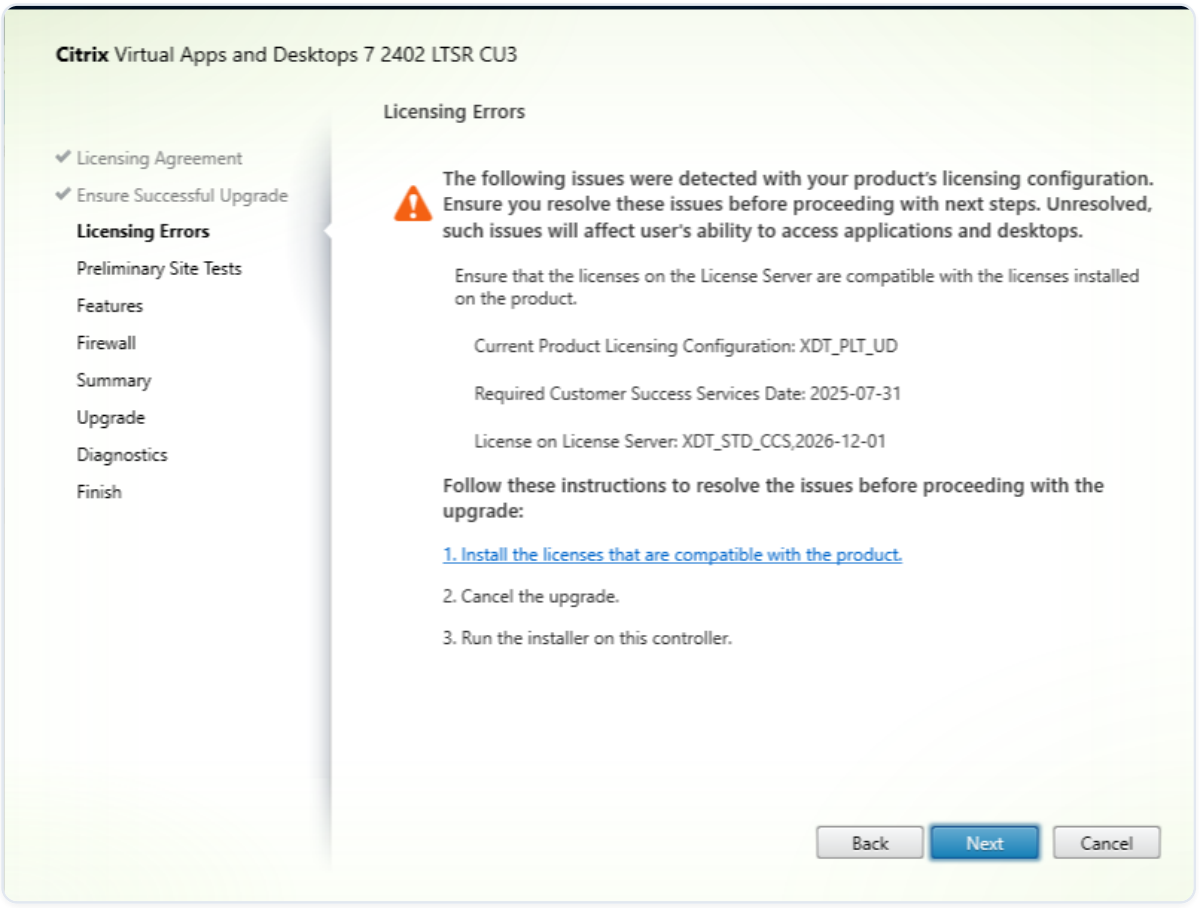
### Considerações importantes para a atualização

Ao atualizar de qualquer versão anterior do Citrix Virtual Apps and Desktops para 2411 e posterior, atualize o License Server para a versão mais recente (versão 11.2.17 build 53100 ou posterior).

- Você recebe os seguintes erros na página de Erros de Licenciamento ao atualizar usando a interface do usuário do metainstaller:
  - Se você não atualizar para a versão mais recente do License Server:




  - Se houver incompatibilidades, como um License Server desatualizado ou indisponibilidade de licenças:




- Se você estiver atualizando usando a linha de comando, execute os seguintes comandos para evitar falha na atualização (assumindo que você esteja dentro da pasta \x64 no ISO montado):

1. Execute o seguinte:

```
\x64\Licensing\CitrixLicensing.exe /quiet
```

Se você copiou os binários de Licenciamento para qualquer uma das unidades locais, execute o seguinte comando:

```
\x64\Licensing\CitrixLicensing.exe /quiet /l install.log
```

2. Execute o seguinte:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
"CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
```

### Desinstalar componentes principais

Durante a atualização, se você instalou o License Server primeiro usando os comandos `\x64\Licensing\CitrixLicensing.exe /quiet` ou `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` e depois instalou os componentes principais, então siga a mesma ordem para desinstalar:

1. Desinstale o License Server usando a linha de comando:

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. Desinstale os componentes usando a GUI ou a linha de comando. Para obter informações, consulte Remover componentes.

Se você desinstalar o License Server e os componentes usando a linha de comando `XenDesktopServerSetup.exe` ou `removeall`, então limpe a entrada do registro e os arquivos restantes.

Para limpar as entradas do registro :

1. Procure pela chave de registro `Citrix Licensing` e exclua essa entrada. Na maioria das vezes, você pode encontrar a entrada no seguinte local:

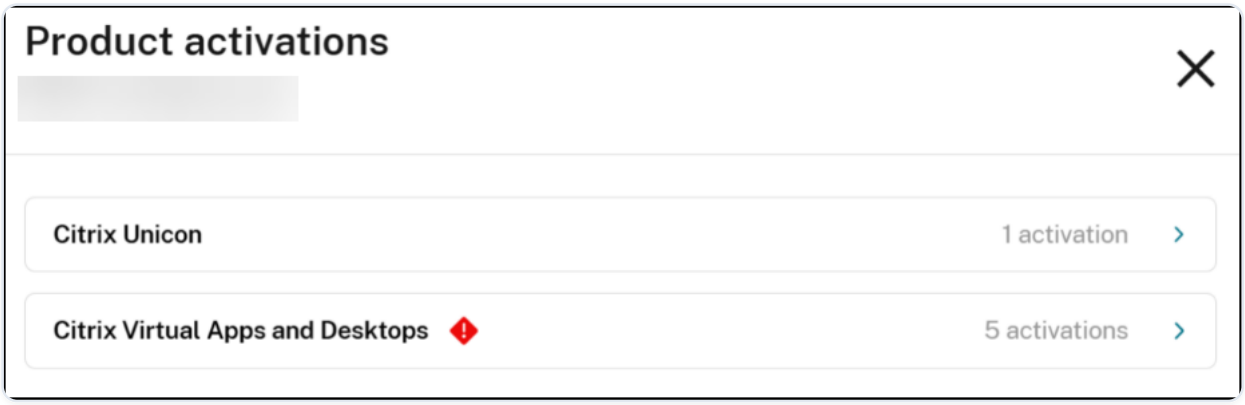
   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. Exclua a pasta apontada pela **Uninstall String** na chave de registro.

## Solução de problemas

Se o status do servidor de licenças estiver mostrando algo diferente de verde no Citrix Cloud, faça o seguinte para entender os detalhes granulares das ativações que podem ter problemas:

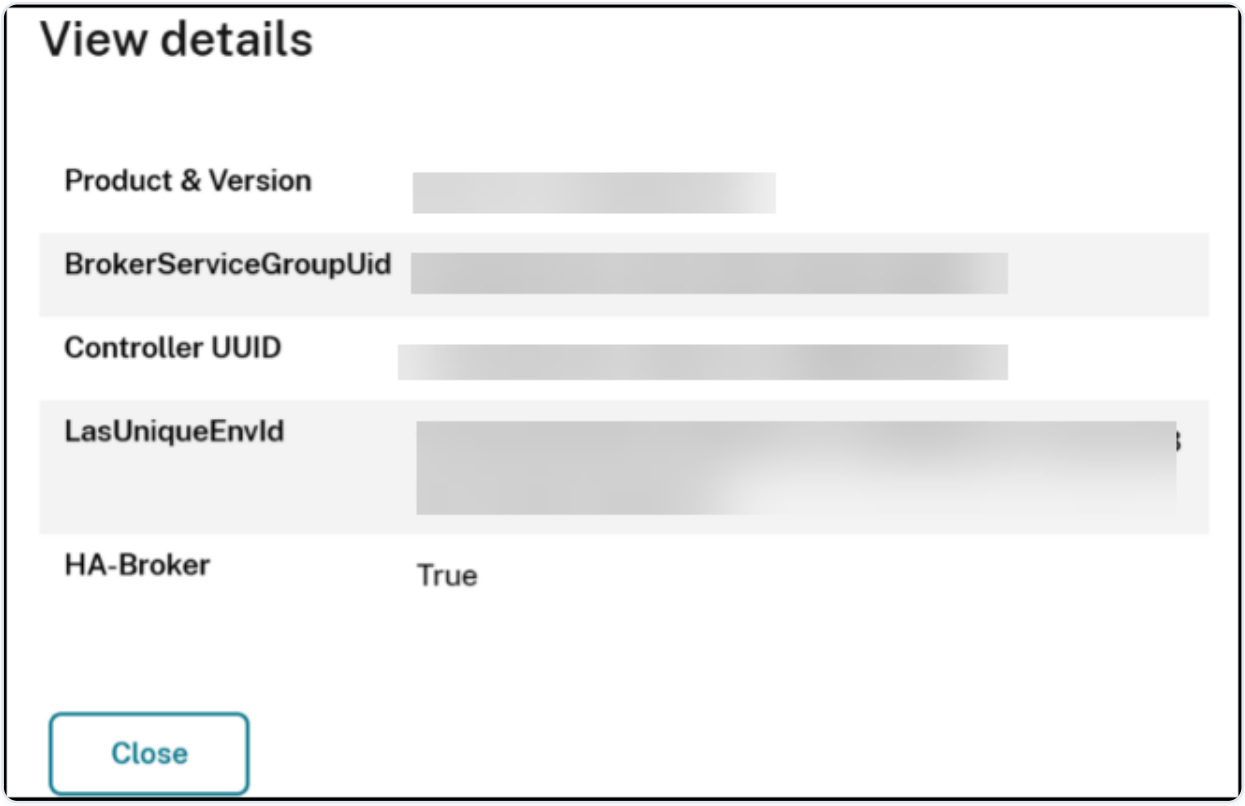
1. No Citrix Cloud, navegar até **Licenciamento > Implantações licenciadas > Servidores de licença**.
2. Clique no botão de expansão **>** em Citrix Virtual Apps and Desktops para ver a lista de Delivery Controllers que foram ativados.




3. Clique em **Ver detalhes** ao lado da ativação para ver os detalhes granulares.

   **ID** é o identificador exclusivo para identificar as ativações.

   Os seguintes detalhes são fornecidos:




- **Produto e Versão**: O Product_Edition_Model e a Data de Gravação que o produto está configurado para usar ao ativar com o LAS. BurnInDate é geralmente a data de lançamento do produto.
- **BrokerServiceGroupUid**: O UID para o Grupo de Serviço do Broker.
- **UUID do Controlador**: O UUID do Delivery Controller.
- **LasUniqueEnvId**: O ID exclusivo da instância fornecida pelo LAS para ativação.
- **HA-Broker**: Verdadeiro ou Falso, indicando se é um broker HA ou um broker principal.

Para mapear os detalhes do host ativado com o host real, execute os seguintes comandos no host.

- `Get-BrokerSite`: Para comparar o valor de **BrokerServiceGroupUid** exibido na tela com a saída `BrokerServiceGroupId` do comando.
- `Get-BrokerController`: Para comparar o valor de **Controller UUID** exibido na tela com a saída UUID do comando.

### Logs do Visualizador de Eventos relacionados a eventos de Licenciamento

| ID DO EVENTO | DESCRIÇÃO |
|---|---|
| 1112 | O Serviço Citrix Broker falhou ao intermediar uma conexão para o usuário com o recurso. A configuração de licenciamento de produto e edição para o site não permite este tipo de recurso. Verifique se a licença correta foi selecionada para este site. |
| 1150 | O Serviço Citrix Broker contatou o servidor de licenças com sucesso. |
| 1151 | O Serviço Citrix Broker não consegue contatar o servidor de licenças. Certifique-se de que o servidor de licenças esteja funcionando corretamente e que os detalhes de identificação do servidor de licenças estejam corretos na configuração do XenDesktop. |
| 1152 | Este site XenDesktop não possui as licenças de produto necessárias presentes no servidor de licenças. Use o Console de Administração de Licenças para adicionar as licenças de produto relevantes ao servidor de licenças. |
| 1153 | A licença deste site XenDesktop expirou. O serviço Citrix Broker solicitará uma nova licença do servidor de licenças. |
| 1154 | Este controlador entrou no modo de cache de licenças porque não conseguiu contatar o servidor de licenças. Você tem 2 hora(s) |

| ID DO EVENTO | DESCRIÇÃO |
| --- | --- |
| | restantes antes que este controlador pare de fornecer sessões de desktop e aplicativo. |
| 1155 | O Serviço Citrix Broker agora parará de fornecer sessões de desktop e aplicativo. Este controlador não está mais ou não conseguiu entrar no modo de cache de licenças devido a falha contínua na comunicação com o servidor de licenças. Certifique-se de que o servidor de licenças esteja funcionando e, se necessário, use o Console de Administração de Licenças para adicionar as licenças relevantes ao servidor de licenças. |
| 1156 | O Serviço Citrix Broker está se comunicando com sucesso com o servidor de licenças. Este controlador não está mais no modo de cache de licenças. |
| 1157 | A versão do servidor de licenças em execução é mais antiga que a versão do Serviço Citrix Broker e, portanto, é incompatível. Atualize seu servidor de licenças ou especifique um local de servidor de licenças com a versão correta em sua configuração XenDesktop. |
| 1158 | O Serviço Citrix Broker detectou que você excedeu o número de licenças disponíveis para este site no servidor de licenças para esta edição. O servidor de licenças concedeu a você uma licença de overdraft. |
| 1159 | O Citrix Broker Service negou uma conexão de desktop porque o número máximo de licenças instaladas para este site foi excedido. Há três licenças instaladas para a edição, mas o número máximo permitido de licenças para esta edição é dois. Remova as licenças relevantes do servidor de licenças para cumprir o limite de licenças. |

| ID DO EVENTO | DESCRIÇÃO |
|---|---|
| 1160 | O serviço de Broker Citrix encontrou um erro interno ao gerenciar licenças. Certifique-se de que o servidor de licenças esteja funcionando corretamente e que os detalhes de identificação do servidor de licenças estejam corretos na configuração do XenDesktop. Reiniciar o serviço de Broker Citrix também pode resolver o problema. Se o problema persistir, reinstale o Citrix XenDesktop Controller. Consulte o artigo CTX126990 da Base de Conhecimento Citrix. |
| 1161 | Erro ao inicializar o licenciamento. Verifique a conectividade do servidor de licenças. |
| 1162 | Erro ao parar o licenciamento. Verifique a conectividade do servidor de licenças. |
| 1163 | Nenhuma licença de conexão disponível. Para resolver, libere licenças fechando sessões que não são necessárias ou adicione mais licenças. |
| 1164 | Erro ao fazer checkout de uma licença de conexão. Verifique a conectividade do servidor de licenças. |
| 1165 | Erro ao fazer check-in de uma licença de conexão. Verifique a conectividade do servidor de licenças. |
| 1166 | Erro ao verificar a disponibilidade da licença. Verifique a conectividade do servidor de licenças. |
| 1167 | Falha ao iniciar o licenciamento. Verifique a conectividade do servidor de licenças. |
| 1168 | Erro ao ler as configurações de notificação do usuário de licenciamento. Verifique a conectividade do servidor de licenças. |

| ID DO EVENTO | DESCRIÇÃO |
| --- | --- |
| 1169 | Este controlador entrou no modo de cache de licença pronto para uso, pois nenhuma licença adequada foi encontrada no servidor de licenças. Você tem 2 hora(s) restantes antes que este controlador pare de fornecer sessões de desktop e aplicativo. |
| 1170 | O Serviço Citrix Broker detectou com sucesso licenças adequadas no servidor de licenças. Este controlador não está mais no modo de cache de licença pronto para uso. |
| 1171 | Nenhum servidor de licenças foi especificado. O Serviço Citrix Broker não pode fornecer desktops e aplicativos aos usuários até que um servidor de licenças válido seja especificado. Você pode especificar um servidor de licenças no Citrix Studio ou com o cmdlet Set-ConfigSite do Citrix PowerShell SDK. |
| 1172 | Erro ao verificar a adequação do servidor de licenças. O serviço Citrix broker recebeu uma resposta inesperada ao verificar se uma máquina é adequada para uso como servidor de licenças. Verifique se a máquina pode ser contatada a partir do controlador e se qualquer firewall na máquina permite conexões do controlador. Se um servidor de licenças estiver instalado na máquina, verifique se ele está configurado e funcionando corretamente. |
| 1173 | Este site do XenDesktop não possui as licenças de inicialização necessárias presentes no servidor de licenças. Use o Console de Administração de Licenças para adicionar as licenças relevantes ao servidor de licenças. |
| 1174 | A edição do produto configurada para este site XenDesktop não oferece suporte a aplicativos; |

| ID DO EVENTO | DESCRIÇÃO |
| --- | --- |
| | os recursos do aplicativo não estarão disponíveis. |
| 1176 | A edição do produto configurada não oferece suporte a máquinas de várias sessões. O registro foi rejeitado. |
| 1177 | A edição do produto configurada não oferece suporte a máquinas de sessão única. O registro foi rejeitado. |
| 1178 | A edição do produto configurada não oferece suporte a RemotePC. O registro foi rejeitado. |
| 1179 | A edição do produto configurada não oferece suporte a máquinas provisionadas em um sistema de nuvem. O registro foi rejeitado. |
| 1180 | A edição do produto configurada para este site XenDesktop não oferece suporte a aplicativos em máquinas de sessão única (SO de estação de trabalho). O recurso do aplicativo teve o lançamento recusado. |
| 1181 | A edição do produto configurada para este site XenDesktop não oferece suporte a aplicativos em máquinas de várias sessões (SO de servidor). O recurso do aplicativo teve o lançamento recusado. |
| 1182 | A edição do produto configurada para este site XenDesktop não oferece suporte a desktops em máquinas de sessão única (SO de estação de trabalho). O recurso de desktop teve o lançamento recusado. |
| 1183 | A edição do produto configurada para este site XenDesktop não oferece suporte a desktops em máquinas de múltiplas sessões (SO de servidor). O recurso de desktop teve seu lançamento recusado. |

| ID DO EVENTO | DESCRIÇÃO |
| --- | --- |
| 1196 | Este controlador entrou em modo de interrupção de licença devido ao esgotamento de todas as licenças utilizáveis no servidor de licenças. Adicione mais licenças para resolver isso. Você tem 2 hora(s) restante(s) antes que este controlador pare de fornecer sessões de desktop e aplicativo. |
| 1197 | O Citrix Broker Service agora deixará de fornecer sessões de desktop e aplicativo. Este controlador não está mais ou não pôde entrar em modo de interrupção de licença devido a licenças insuficientes no servidor de licenças. Use o Console de Administração de Licenças para adicionar as licenças relevantes ao servidor de licenças. |
| 1198 | O Citrix Broker Service está consumindo licenças com sucesso do servidor de licenças. Há licenças suficientes no servidor para satisfazer a demanda atual. Este controlador não está mais em modo de interrupção de licença causado pelo esgotamento de licenças. |
| 1199 | O Citrix Broker Service agora deixará de fornecer sessões de desktop e aplicativo. Este controlador não está mais ou não pôde entrar em modo de cache de licença, pois nenhuma licença está instalada no servidor de licenças. Use o Console de Administração de Licenças para adicionar as licenças relevantes ao servidor de licenças. |
| 1205 | Sua manutenção de software expirou. Seu ambiente Citrix não é atualmente suportado. Verifique seu servidor de licenças para licenças expiradas e remova-as. Há um modo de cache de licença de 30 dias antes que os usuários comecem a receber mensagens de aviso. |

| ID DO EVENTO | DESCRIÇÃO |
|---|---|
| 1206 | O hash do certificado de licença é inválido. O hash do seu certificado de licença Citrix é inválido. |
| 1300 | O Serviço de Broker Citrix deixará de fornecer sessões de desktop e aplicativo. Há um problema com o relógio do sistema do servidor de licenças. |
| 1301 | Os problemas com o relógio do sistema do servidor de licenças foram corrigidos. O Serviço de Broker Citrix retomará a operação normal. |
| 1302 | Este controlador falhou novamente ao verificar ou retirar uma licença de conexão. Falhas detectadas anteriormente ainda existem. Para evitar o registro excessivo de eventos, o serviço está suprimindo mensagens relacionadas (ID de evento 1163, 1164, 1165) até que o problema seja resolvido. As tentativas de licenciamento continuarão. |
| 1303 | Este controlador não está mais suprimindo mensagens relacionadas (ID de evento 1163, 1164, 1165). |
| 1304 | O Serviço de Broker Citrix contatou o LAS com sucesso. |
| 1305 | O Serviço de Broker Citrix não consegue contatar o LAS. Certifique-se de que o LAS esteja funcionando corretamente e que os detalhes de identificação do LAS estejam corretos na configuração do XenDesktop. |

### Mais informações

Para obter informações sobre como verificar o estado do LAS de um site ou verificar se um site está no modo de cache de licenças, consulte:

- Como posso verificar o estado do LAS de um site?
- Como posso verificar se um site está no modo de cache de licenças?

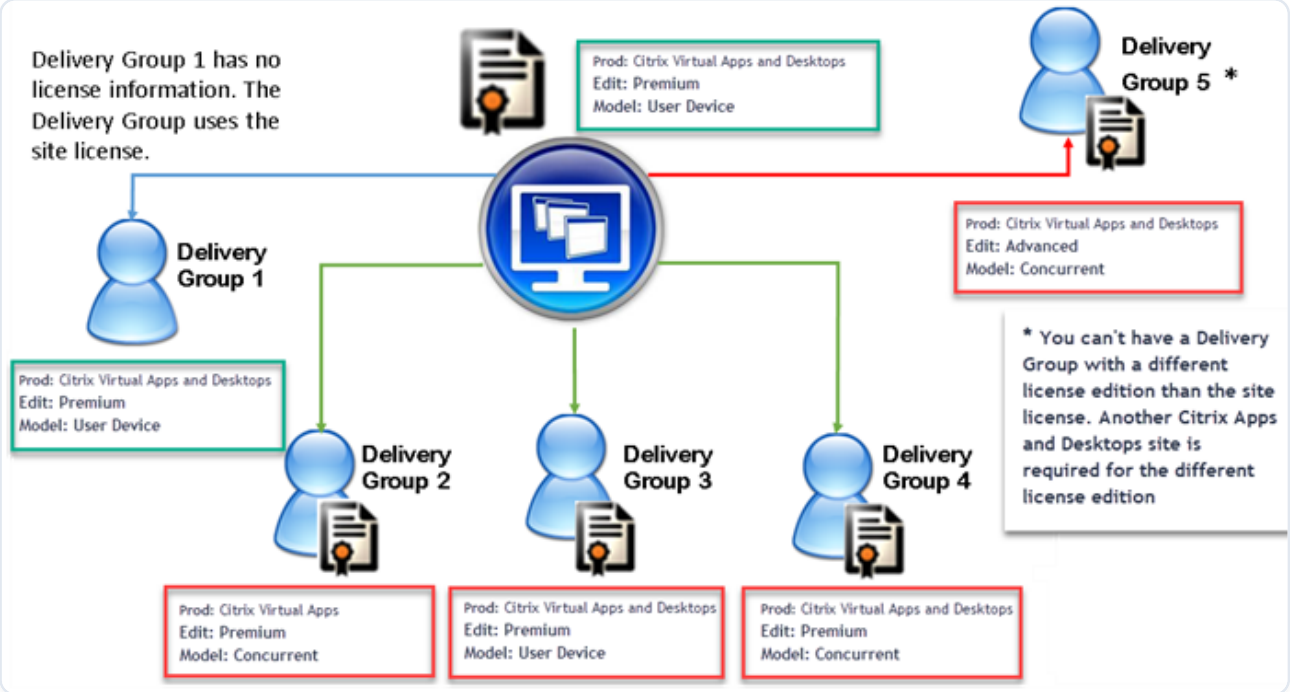
Para obter informações detalhadas sobre os comandos, consulte:

- Get-BrokerController
- Get-ConfigSite

## Licenciamento multitipo

O licenciamento multitipo suporta o consumo de diferentes tipos de licença para grupos de entrega em um único site do Citrix Virtual Apps and Desktops. **Tipo** é uma combinação única de ID do Produto (XDT ou MPS) e Modelo (UserDevice ou Concurrent). Os grupos de entrega devem usar a mesma Edição do Produto (PLT/Premium ou ENT/Advanced) conforme configurado no nível do site. Esteja ciente das considerações especiais no final deste artigo ao configurar o licenciamento multitipo para suas implantações do Citrix Virtual Apps and Desktops.

Se o licenciamento multitipo não estiver configurado, diferentes tipos de licença podem ser usados apenas quando configurados para sites separados. Os grupos de entrega usam a licença do site. Para limitações importantes de notificação quando o licenciamento multitipo está configurado, consulte Considerações especiais.




Para determinar os grupos de entrega que consomem os diferentes tipos de licenças, use estes cmdlets do Broker PowerShell:

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Para instalar licenças, use:

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

As datas dos Customer Success Services são específicas para cada arquivo de licença e para cada produto e modelo. Grupos de entrega configurados de forma diferente podem ter datas de Customer Success Services diferentes entre si.

### Considerações especiais

O licenciamento multitipo tem funcionalidade diferente do licenciamento regular do Citrix Virtual Apps and Desktops™.

Não há alertas e notificações do Director ou Studio para grupos de entrega configurados para usar um tipo que difere da configuração do site:

- Nenhuma informação ao se aproximar dos limites de licença ou do acionamento ou expiração do modo de intermitência de licença.
- Nenhuma notificação quando um grupo específico tem um problema.

Os grupos de entrega configurados para licenças de vários tipos consomem APENAS esse tipo de licença e não retornam à configuração do site quando totalmente consumidos.

Embora os nomes das edições de licença Citrix Virtual Apps Standard e Citrix Virtual Desktops™ Standard indiquem que ambos são Standard, eles não são a mesma edição. O licenciamento de vários tipos não está disponível com as licenças Citrix Virtual Apps Standard e Citrix Virtual Desktop Standard.

### Matriz de compatibilidade de licenças

Esta tabela detalha nomes de produtos antigos, novos nomes de produtos e os nomes de recursos associados. As quatro colunas de compatibilidade especificam quais combinações de produto e modelo de licença são compatíveis para licenciamento de vários tipos. CCU e CCS significam licenças simultâneas e UD são licenças de usuário/dispositivo.

| Old Name | New Name | Feature | Multi-type licensing compatibility | | | |
|---|---|---|---|---|---|---|
| | | | STD | ADV | ENT | PLT |
| Citrix XenApp Standard | Citrix XenApp Standard | MPS_STD_CCU | X | | | |
| Citrix XenApp Advanced | Citrix Virtual Apps Standard | MPS_ADV_CCU | | X | | |
| Citrix XenApp Enterprise | Citrix Virtual Apps Advanced | MPS_ENT_CCU | | | X | |
| Citrix XenApp Platinum | Citrix Virtual Apps Premium | MPS_PLT_CCU | | | | X |
| Citrix XenDesktop VDI Edition (XDT-U) | Citrix Virtual Desktops Standard- Per User/Device | XDT_STD_UD | X | | | |
| Citrix XenDesktop VDI Edition (XDT-C) | Citrix Virtual Desktops Standard - Concurrent | XDT_STD_CCS | X | | | |
| Citrix XenDesktop Enterprise Edition (XDT-C) | Citrix Virtual Apps and Desktops Advanced - Concurrent | XDT_ENT_CCS | | | X | |
| Citrix XenDesktop Enterprise Edition (XDT-U) | Citrix Virtual Apps and Desktops Advanced - Per User/Device | XDT_ENT_UD | | | X | |
| Citrix XenDesktop Platinum Edition (XDT-C) | Citrix Virtual Apps and Desktops Premium - Concurrent | XDT_PLT_CCS | | | | X |
| Citrix XenDesktop Platinum Edition (XDT-U) | Citrix Virtual Apps and Desktops Premium - Per User/Device | XDT_PLT_UD | | | | X |

## SDK do Broker PowerShell

O objeto **DesktopGroup** possui estas duas propriedades que você pode manipular usando os cmdlets New-BrokerDesktopGroup e Set-BrokerDesktopGroup associados.

| NOME | VALOR | RESTRIÇÃO |
|---|---|---|
| LicenseModel | Um parâmetro (Concurrent ou UserDevice) que especifica o modelo de licenciamento para o grupo. Se nenhum for especificado, o modelo de licença de todo o site será usado. | Se a alternância de recurso estiver desativada, a tentativa de definir uma propriedade falhará. |
| ProductCode | Uma string de texto de XDT (para Citrix Virtual Desktops) ou MPS (para Citrix Virtual Apps™) especificando o ID do produto de licenciamento para o grupo. Se nenhum for especificado, o código do produto de todo o site será usado. | Se a alternância de recursos estiver desabilitada, a tentativa de definir uma propriedade falha. |

Para obter mais informações sobre LicenseModel e ProductCode, consulte about_Broker_Licensing.

### New-BrokerDesktopGroup

Cria um grupo de desktops para gerenciar a intermediação de grupos de desktops. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`.

### Set-BrokerDesktopGroup

Desativa ou ativa um grupo de desktops de broker existente ou altera suas configurações. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`

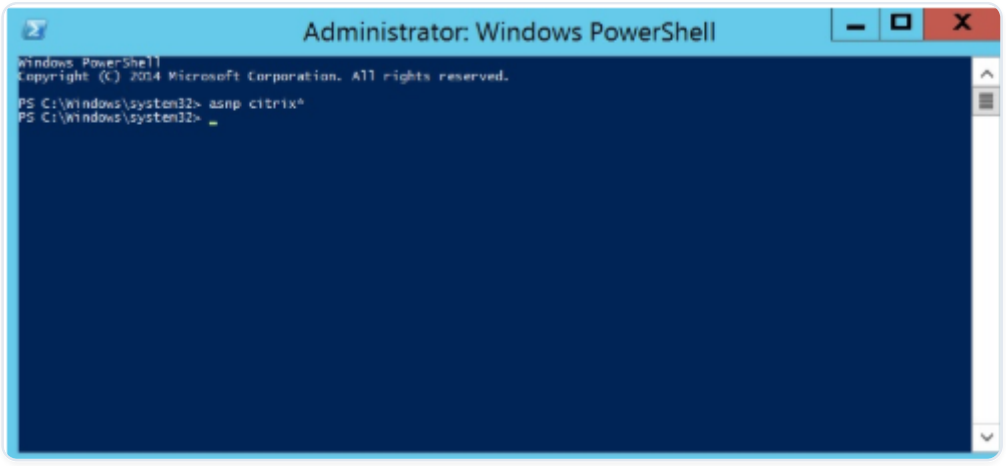
### Get-BrokerDesktopGroup

Recupera grupos de desktops que correspondem aos critérios especificados. A saída do cmdlet Get-BrokerDesktopGroup inclui as propriedades **ProductCode** e **LicenseModel** do grupo. Se as propriedades não tiverem sido definidas usando New-BrokerDesktopGroup ou Set-BrokerDesktopGroup, valores nulos serão retornados. Se nulo, o modelo de licença e o código do produto de todo o site serão usados. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`.

## Configurar diferentes produtos e modelos de licença por grupo de entrega

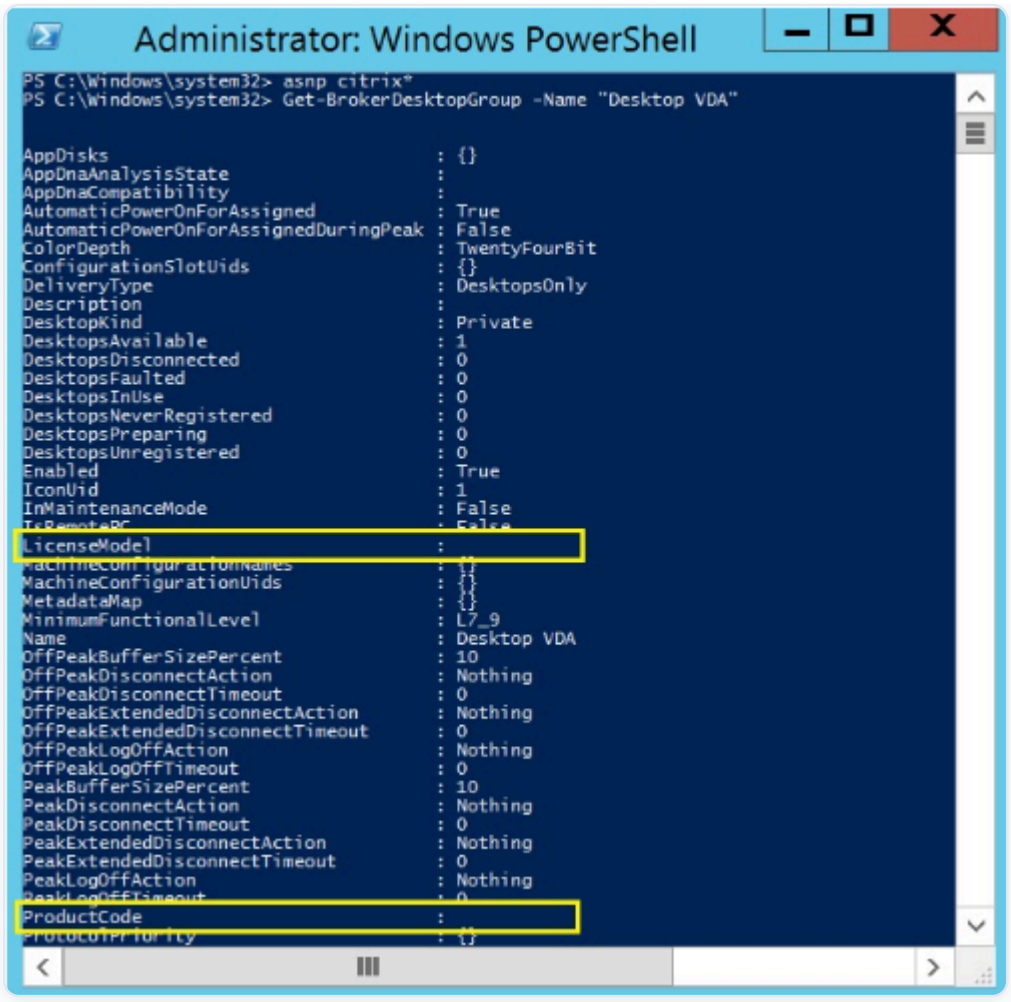
> **Nota:**
>
> Não é possível configurar dois ou mais tipos diferentes de produtos, edições ou modelos de licença em um único grupo de entrega. Caso você tenha diferentes tipos de produtos, edições ou modelos de licença, configure-os em grupos de entrega separados.

1. Abra o PowerShell com direitos administrativos e adicione o snap-in do Citrix.

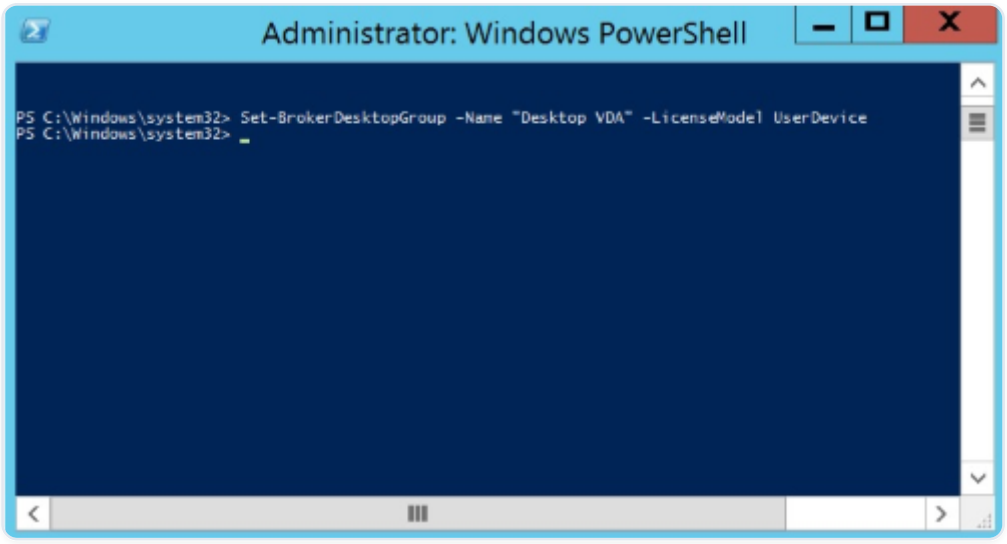


2. Execute o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para visualizar a configuração de licença atual. Encontre os parâmetros **LicenseModel** e **ProductCode**. Se você não configurou esses parâmetros antes, eles podem estar em branco.

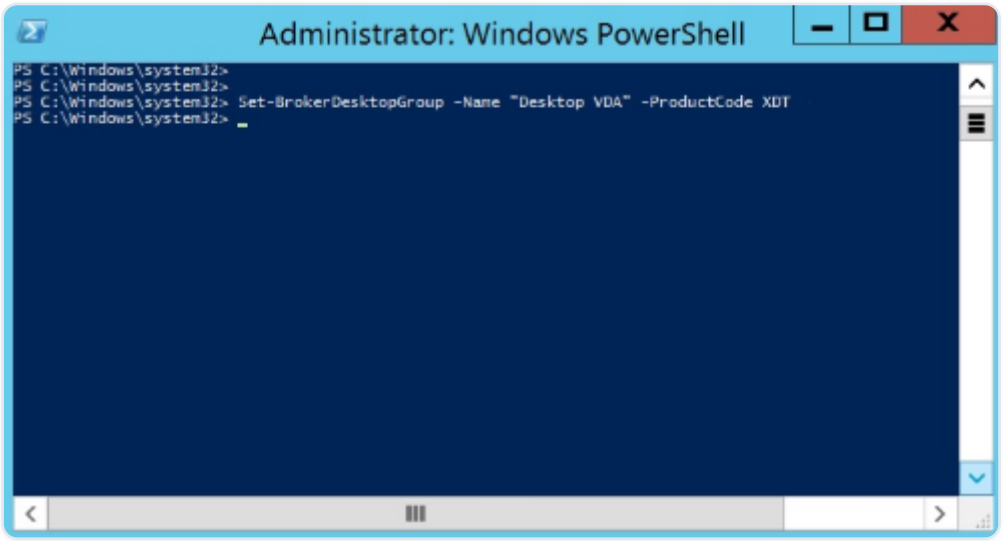
> **Nota:**
>
> Se um grupo de entrega não tiver informações de licença definidas, ele usará como padrão **Licença de site no nível do site**.



3. Altere o modelo de licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**.

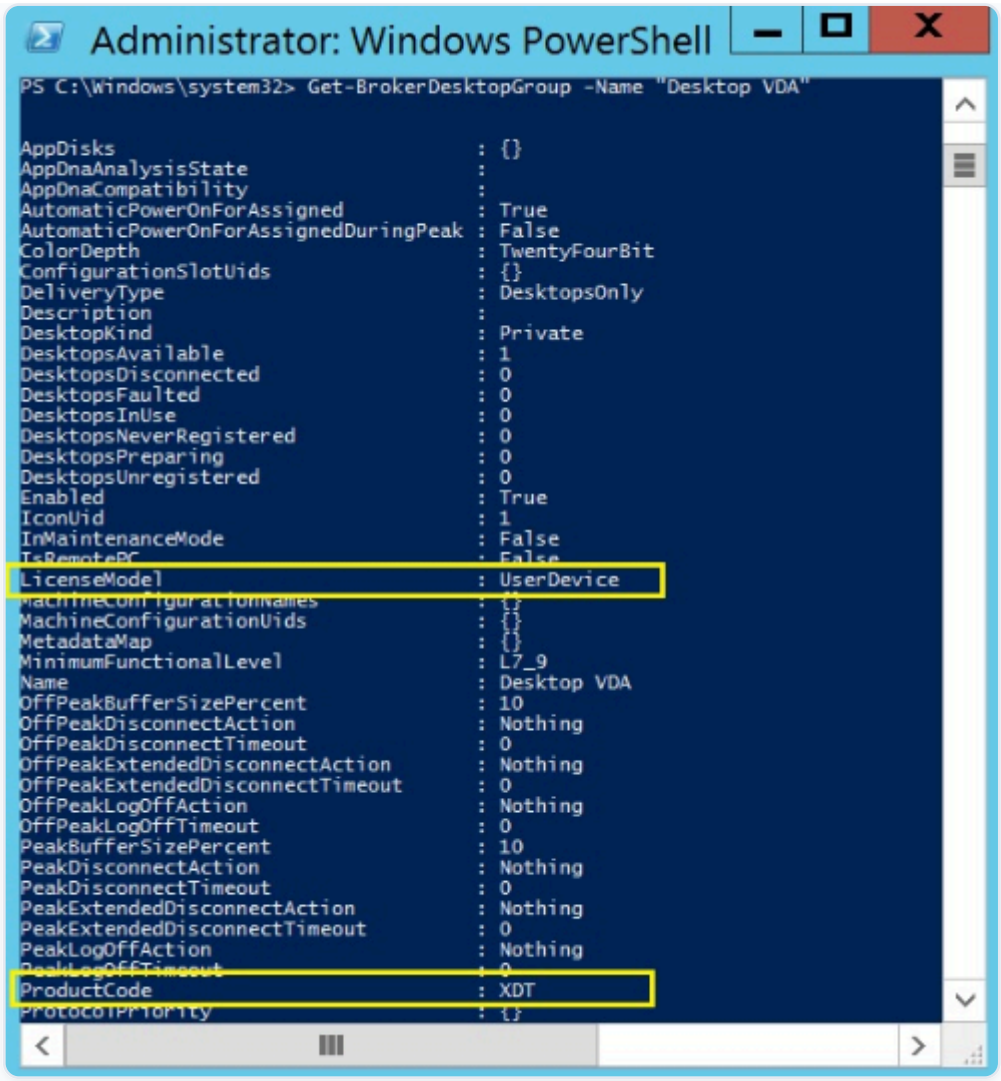



4. Altere o produto da licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**.



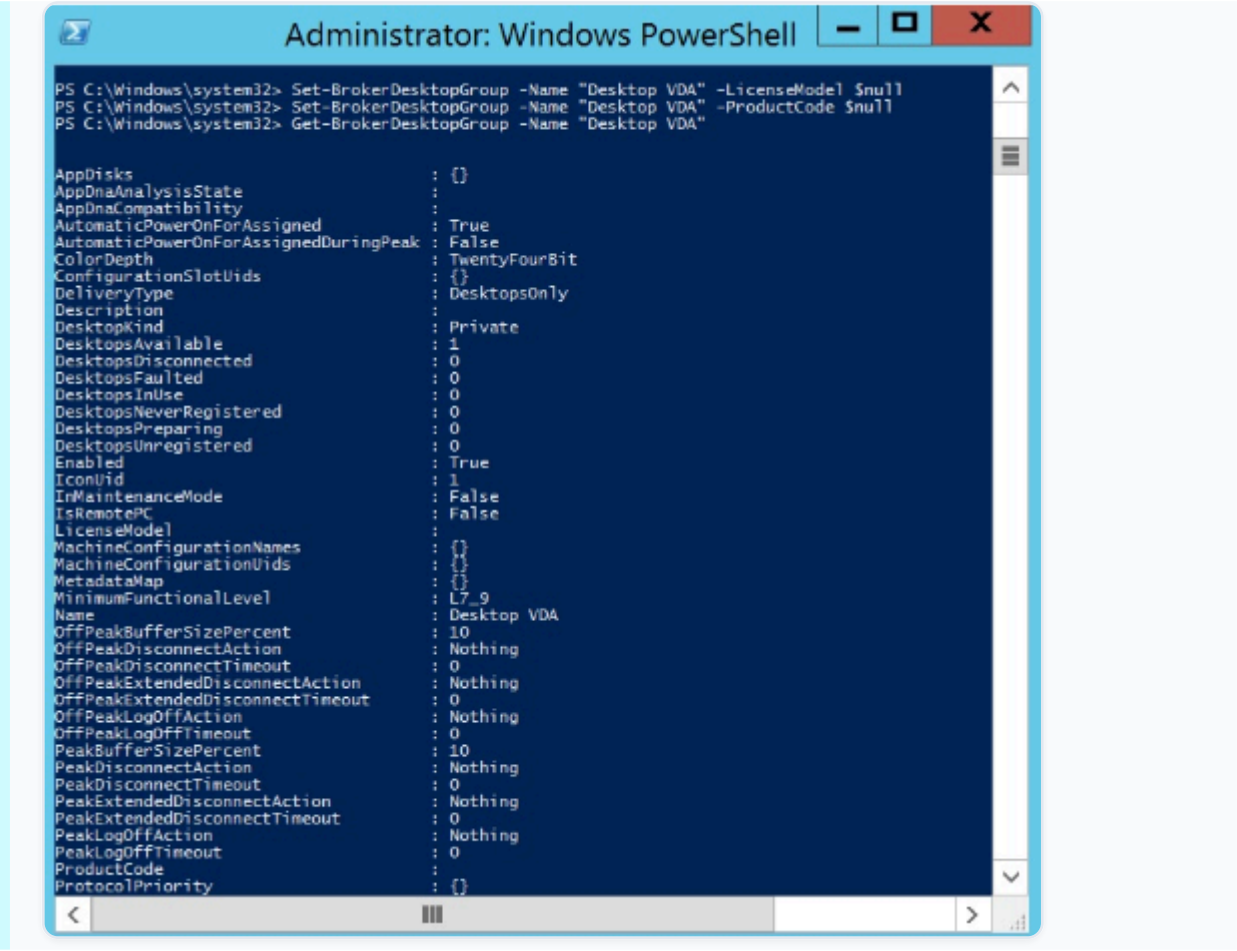

5. Insira o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para validar as alterações.

> **Nota:**
>
> Não é possível misturar e combinar edições no mesmo site. Por exemplo, licenças Premium e Advanced. Vários sites são necessários se você tiver licenças com edições diferentes.




6. Remova a configuração da licença executando os mesmos comandos **Set-BrokerDesktopGroup** descritos nas etapas anteriores e defina o valor como **$null**.

> **Nota:**
>
> O Studio não exibe a configuração da licença para cada grupo de entrega. Use o PowerShell para visualizar a configuração atual.




### Exemplo

Este exemplo de cmdlet PowerShell ilustra a configuração de licenciamento multi-tipo para dois grupos de entrega existentes e cria e configura um terceiro grupo de entrega.

Para ver o produto da licença e o modelo de licença associados a um grupo de entrega, use o cmdlet do PowerShell **Get-BrokerDesktopGroup**.

1. Configuramos o primeiro grupo de entrega para XenApp® e Concorrente.

   **Set-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Apps Premium Concorrente" -ProductCode MPS -LicenseModel Concurrent**

2. Configuramos o segundo grupo de entrega para XenDesktop® e Concorrente.

   **Set-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Desktops Premium Concorrente" -ProductCode XDT -LicenseModel Concurrent**

3. Criamos e configuramos o terceiro grupo de entrega para XenDesktop e UserDevice.

**New-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Desktops Premium UsuárioDispositivo" -PublishedName "MeuDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

# Elementos de dados de telemetria do Citrix Virtual Apps and Desktops™

## Broker

### Sessão

#### CABEÇALHOS

| CHAVE | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| Versão | Indica a versão do evento de uso de telemetria. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | d4ce7919-5d80-44de-a8fa-102923fe0ead |
| Tipo | Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem. | SendBrokerTelemetryData |
| st | Indica o carimbo de data/hora quando o evento é gerado no Broker. | 2011-08-12T20:17:46.384Z |
| produção | Identifica o produto de origem e a implantação do evento de uso. | XenDesktop.Broker |
| prodVer | Indica a versão do produto Citrix DaaS/ | 7.25.0.0 |

| CHAVE | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | Citrix Virtual Apps and Desktops. | |
| usuário | Identifica o ID do Usuário para identificar de forma exclusiva um usuário que inicia o lançamento da sessão. | fullName: C648FE671A44B3F7 samName:C758LH671A44B3F7<br><br>Nome Principal do Usuário: C7948FE671A44B3F7<br><br>userLicenseId:C265FE671A44B3F7<br><br>userSid: C097FE671A44B3F7 |
| locatário -> ID | Indica o ID do Cliente da conta Citrix Cloud™. Para a implantação local, o valor é sempre "CitrixOnPremises". | joj1mh0598tj |
| dvc para dvcId | Indica o ID do dispositivo para identificar exclusivamente um dispositivo de onde o lançamento da sessão é iniciado. | AE18C4D5 |
| dvc para dvcName | Indica o nome amigável para o dispositivo. | C758LH671A44B3F7 |

### CARGA ÚTIL

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| appProtectionKeyLoggingRequired | Indica se a sessão é iniciada com a Proteção de Registro de Teclas ativada. | Falso |
| appProtectionScreenCaptureRequired | Indica se a sessão é iniciada com a Proteção de Captura de Tela ativada. | Falso |
| cspTenantCustomerId | Indica o ID do Cliente de uma conta Citrix Cloud de um locatário CSP. Para implantações locais, este campo é deixado em branco se o ID do cliente não estiver disponível. | 6c2vtxgxyftt |
| isAnonymousUser | Indica se uma sessão não autenticada é iniciada. | Falso |
| licenseActivityTimeStamp | Indica o carimbo de data/hora em que o payload é gerado. | 2011-08-12T20:17:46.384Z |
| licenseActivityType | Indica o tipo de evento de licenciamento. Este campo indica se o tipo de evento de licenciamento é para ação de atribuição ou liberação. | Conectar |
| licenseModel | Indica o modelo de licença da implantação. | UserDevice |
| productEdition | Indica a edição do produto da implantação. | Premium ou Avançado |
| productId | Indica o ID do produto do produto na implantação. | CAVDS |
| protocolo | Indica o protocolo usado para iniciar a sessão. | HDX™ |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| sessionKey | Indica um identificador exclusivo para a sessão. | uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2 |
| sessionSupport | Indica o tipo de suporte da sessão. | SingleSession |
| sessionType | Indica o tipo de sessão. | Aplicativo |
| versão | Indica a versão do payload. | 1.3 |
| workerSid | Indica um identificador exclusivo para o VDA usado na sessão.**O valor é embaralhado.** | 1E5LH671A44B3F7 **(sempre embaralhado)** |
| isWindows365 | Indica se a sessão é iniciada para o Windows 365. | Verdadeiro |
| entitlementType | Indica o tipo de direito de licença do Cliente. | Produção |
| siteId | Indica um identificador exclusivo para o site. | a35647d0-901c-4477-87e0-dcd781d455f4 |
| desktopGroupId | Indica um identificador exclusivo para o Grupo de Área de Trabalho ou de Entrega. | e9d859dc-1bfc-4b3e-bad3-41806bb4e694 |
| clientType | Indica o tipo de aplicativo Citrix Workspace™. | Windows |
| clientVersion | Indica a versão do aplicativo Citrix Workspace. | 23.5.1.83 |
| workerCloudType | Indica o tipo de nuvem pública usado para provisionamento de VDA. | Azure |
| enabledFeatures | Indica os recursos que estão habilitados para a sessão. Por exemplo, em uma sessão | 66 |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | onde `AppProtectionScreenCaptureRequired` e `SessionRecording` estão habilitados, o valor deste campo é 66. | |
| isEvents | Indica as falhas críticas em {{page.lic}}. | Não foi possível criar o banco de dados ST. |
| heartBeatTime | Indica o tempo de pulsação do servidor de licenças para o CIS ou Citrix Analytic Service. | 1689058813 |

### Embaralhar dados de telemetria de licenciamento

Considerando a sensibilidade das informações enviadas na telemetria de licença, a Citrix oferece uma opção para embaralhar os dados.

A tabela a seguir lista os dados que podem ser embaralhados:

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| usuário | Identifica o ID do Usuário para identificar exclusivamente um usuário que inicia o lançamento da sessão. | • fullName: `C648FE671A44B3F7`<br>• samName: `C758LH671A44B3F7`<br>• nome principal do usuário: `C7948FE671A44B3F7`<br>• userLicenseId: `C265FE671A44B3F7` |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | | • userSid: `C097FE671A44B3F7` |
| dvc para dvcName | Indica o nome amigável para o dispositivo. | `C758LH671A44B3F7` |
| workerSid | Indica um identificador exclusivo para o VDA usado na sessão. | `1E5LH671A44B3F7` |
| AdminLoginList | Indica a lista de SamAccountName de administradores exclusivos | `{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}` |

Para habilitar ou desabilitar a ofuscação, execute os seguintes comandos PowerShell no Delivery Controller.

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando para habilitar ou desabilitar a ofuscação:

   Por padrão, o valor é `0`, ou `false`, o que desabilita a ofuscação dos dados de telemetria de licença.

   Para habilitar:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

   **Observação:**

> Para um cliente Citrix Service Provider™ (CSP), a ofuscação é desabilitada por padrão.

> Depois de habilitar a ofuscação, você pode desabilitá-la usando o seguinte comando:

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $false
```

## Elementos de dados de telemetria do Citrix Virtual Apps and Desktops 2402 LTSR CU1

### Broker

#### Uso

CABEÇALHOS

| CHAVE | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| Versão | Indica a versão do evento de telemetria. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | d4ce7919-5d80-44de-a8fa-102923fe0ead |
| tipo | Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso na nuvem. | SendBrokerTelemetryData |
| st | Indica o carimbo de data/hora quando o evento é gerado no Broker. | 2011-08-12T20:17:46.384Z |
| Produto | Identifica o produto de origem e a | XenDesktop.Broker (Cloud) |

| CHAVE | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| | implantação do evento de uso. | OnPrem.Broker (OnPrem) |
| prodVer | Indica a versão do produto Citrix DaaS/ Citrix Virtual Apps and Desktops. | 7.25.0.0 |

### CARGA ÚTIL

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| TotalPublishedApps | Indica o número total de aplicativos publicados. | 10 |
| TotalPublishedDesktops | Indica o número total de Desktops publicados. | 10 |
| VDAs.Total | Indica o número total de VDAs. | 10 |
| VDAs.OSTypes | Indica o número total de VDAs por tipos de SO, como Windows, Linux e Mac. | 10 |
| VDAs.OSVersions | Indica o número total por versões de SO, como Windows 10, 11, 2022, 2019. | 10 |
| VDAs.HostingLocations.Azure | Indica o número de VDAs para cada local de hospedagem suportado, como Azure, AWS, GCP, Nutanix, VMWare, XenServer e HyperV. | 10 |
| VDAs.HostingLocations.AWS | | |
| VDAs.HostingLocations.Nutanix | | |
| VDAs.HostingLocations.VMWare | | |
| VDAs.HostingLocations.XenServer | | |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| VDAs.HostingLocations.HyperV | | |
| VDAs.ProvisionedMethod.MCS | Indica o número de máquinas provisionadas pelo Machine Creation Service (MCS). | 10 |
| VDAs.ProvisionedMethod.ManualOr3P | Indica o número de máquinas provisionadas manualmente ou por 3P. | 10 |
| VDAs.SessionSupport.StaticSingle | Indica o número de máquinas com sessão única atribuída estaticamente. | 10 |
| VDAs.SessionSupport.DynamicSingle | Indica o número de máquinas com sessão única atribuída dinamicamente. | 10 |
| VDAs.SessionSupport.Multi | Indica o número total de máquinas multi-sessão. | 10 |
| VDAs.RemotePCAccess.Windows | Indica o número de máquinas de Acesso Remoto a PC por tipo de SO (Win, Mac, Linux). | 10 |
| VDAs.RemotePCAccess.Linux | Idem | Idem |
| VDAs.RemotePCAccess.MacOS | Idem | |
| VDAs.ActiveSessionRecordingAgents | Indica o número de VDAs com agentes de gravação de sessão ativos. | 5 |
| VDAs.Subscriptions | Indica o número de assinaturas de nuvem pública de VDAs. | 2 |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| VDAs.LocationTypes | Indica o número de tipos de localização de VDAs. | 2 |
| AutoScale.DGWithAutoscaleEnabled | Indica o número de grupos de entrega com **Autoscale** habilitado. | 2 |
| AutoScale.TotalMachinesCtrlByAutoscale | Indica o número de máquinas controladas pelo autoscale. | 5 |
| AutoScale.VerticalAutoscaleEnabledByDGandSite | Indica o número de máquinas com **Vertical Autoscale** habilitado por DG e Site. | 2 |
| AutoScale.TaggedBasedAutoscaledDG | Indica o número de grupos de entrega com autoescala baseada em tags. | 2 |
| DeliveryGroup.TotalRebootSchedulesEnabled | Indica o número de grupos de entrega com **Reboot Schedules** habilitados. | 2 |
| DeliveryGroup.Total | Indica o número total de grupos de entrega. | 10 |
| Policy.TotalPolicySets | Indica o número de conjuntos de políticas. | 3 |
| Policy.TotalPolicies | Indica o número de políticas de grupo. | 2 |
| Policy.TotalPolicySettings | Indica o número de configurações de grupo. | 2 |
| PublishedPackageApps.AppVSingleAdmin | Indica o número total de aplicativos empacotados publicados no modo AppV Single Admin. | 2 |
| PublishedPackageApps.AppVDualAdmin | Indica o número total de aplicativos empacotados | 2 |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| | publicados no modo AppV Dual Admin. | |
| PublishedPackageApps.Msix | Indica o número total de aplicativos empacotados publicados no modo MSIX. | 2 |
| PublishedPackageApps.AppAttach | Indica o número total de aplicativos empacotados publicados no modo AppAttach. | 2 |
| PublishedPackageApps.FlexApp | Indica o número total de aplicativos empacotados publicados no modo FlexApp. | 2 |

### Sessão

#### CABEÇALHOS

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| ver. | Indica a versão do evento de uso de licença. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | d4ce7919-5d80-44de-a8fa-102923fe0ead |
| tipo | Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem. | Cloud.Licensing |
| st | Indica o carimbo de data/hora em que o evento é gerado no Broker. | 2011-08-12T20:17:46.384Z |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| produção | Identifica o produto de origem e a implantação do evento de uso. | XenDesktop.Broker (Cloud)<br>OnPrem.Broker (OnPrem) |
| prodVer | Indica a versão do produto Citrix DaaS ou Citrix Virtual Apps and Desktops. | 7.25.0.0 |
| usuário | Identifica o ID do Usuário para identificar unicamente um usuário que inicia o lançamento da sessão. **O valor é embaralhado.** | fullName: C648FE671A44B3F7 **(sempre embaralhado)**<br>samName:C758LH671A44B3F7 **(sempre embaralhado)**<br><br>upn: C7948FE671A44B3F7 **(sempre embaralhado)**<br><br>userLicenseId:C265FE671A44B3F7 **(sempre embaralhado)**<br><br>userSid: C097FE671A44B3F7 **(sempre embaralhado)** |
| locatário -> ID | Indica o ID do Cliente da conta Citrix Cloud. Para a implantação local, este campo não é | joj1mh0598tj |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | aplicável e não possui valor. | |
| disp. -> ID disp. | Indica o ID do dispositivo para identificar unicamente um dispositivo de onde o lançamento da sessão é iniciado. | AE18C4D5 |
| dispositivo -> Nome do dispositivo | Indica o nome amigável para o dispositivo. **O valor é embaralhado.** | C758LH671A44B3F7 **(sempre embaralhado)** |

### CARGA ÚTIL

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| appProtectionKeyLoggingRequired | Indica se a sessão é iniciada com a Proteção de Registro de Teclas ativada. | Falso |
| appProtectionScreenCaptureRequired | Indica se a sessão é iniciada com a Proteção de Captura de Tela ativada. | Falso |
| cspTenantCustomerId | Indica o ID do Cliente de uma conta Citrix Cloud de um locatário CSP. Para a implantação local, este campo não é aplicável e não possui valor. | 6c2vtxgxyftt |
| isAnonymousUser | Indica se uma sessão não | Falso |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | autenticada é iniciada. | |
| licenseActivityTimeStamp | Indica o carimbo de data/hora quando a carga útil é gerada. | 2011-08-12T20:17:46.384Z |
| licenseActivityType | Indica o tipo de evento de licenciamento. Este campo indica se o tipo de evento de licenciamento é para ação de atribuição ou liberação. | Conectar |
| licenseModel | Indica o modelo de licença da implantação. | UserDevice |
| productEdition | Indica a edição do produto da implantação. | Premium |
| productId | Indica o ID do produto do produto na implantação. | CAVDS |
| protocolo | Indica o protocolo usado para iniciar a sessão. | HDX |
| sessionKey | Indica um identificador exclusivo para a sessão. | uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2 |
| sessionSupport | Indica o tipo de suporte da sessão. | SingleSession |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| sessionType | Indica o tipo de sessão. | Application |
| versão | Indica a versão do payload. | 1.3 |
| workerSid | Indica um identificador exclusivo para o VDA usado para a sessão.**O valor é embaralhado.** | 1E5LH671A44B3F7 **(sempre embaralhado)** |
| isWindows365 | Indica se a sessão é iniciada para o Windows 365. | Verdadeiro |
| entitlementType | Indica o tipo de direito de licença do Cliente. | Produção |
| siteId | Indica um identificador exclusivo para o site. | a35647d0-901c-4477-87e0-dcd781d455f4 |
| desktopGroupId | Indica um identificador exclusivo para o Grupo de Desktops ou de Entrega. | e9d859dc-1bfc-4b3e-bad3-41806bb4e694 |
| clientType | Indica o tipo de aplicativo Citrix Workspace. | Windows |
| clientVersion | Indica a versão do aplicativo Citrix Workspace. | 23.5.1.83 |
| workerCloudType | Indica o tipo de nuvem pública usado para o | Azure |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | provisionamento de VDA. | |
| enabledFeatures | Indica os recursos que estão habilitados para a sessão. Por exemplo, em uma sessão onde `AppProtectionScreenCaptureRequired` e `SessionRecording` estão habilitados, o valor deste campo é 66. | 66 |
| launchRequestSource | Registra o produto usado para solicitar o lançamento. Pode ser On-prem StoreFront™ ou Cloud StoreFront. | 0 (StoreFront ou 3P)<br>1 (Workspace) |
| isEvents | Indica as falhas críticas em {{page.lic}}. | Não foi possível criar o banco de dados ST. |
| heartBeatTime | Indica o tempo de pulsação do servidor de licenças para o CIS ou Citrix Analytic Service. | 1689058813 |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| vdaTelemetry | Indica o payload que é capturado para App Layering, User Personalization Layer, User Profile management, Workspace Environment Management™, e recursos HDX. | vdaTelemetry<br>SessionTelemetry<br><br>CPM_feature: 32<br><br>HDX1: 66<br><br>HDX2: 0<br><br>MachineTelemetry<br><br>AL_productVersion: 23.12.0.1001<br><br>UPL_isEnabled: 1<br><br>CPM_version: 22.3.4000<br><br>wem_enableMethod : 1 |
| | | wem_agentVersion: 2402.1 |

## Studio

### Uso

#### CABEÇALHOS

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| versão | Indica a versão do evento de uso da licença. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | 8c2e20a5-ca3f-4401-ad69-d037933c40a0 |
| tipo | Indica o tipo de evento usado pelo Citrix Analytic Service | Studio.Usage |

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| | para identificar eventos de uso da nuvem | |
| st | Indica o carimbo de data/hora quando o evento é gerado no Studio. | 2024-03-22T01:32:23.4056195Z |
| produto | Identifica o produto de origem e a implantação do evento de uso. | XenDesktop.Studio |
| prodVer | Indica a versão do produto Citrix DaaS/Citrix Virtual Apps and Desktops | 7.42.0.0 |

### CARGA ÚTIL

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| AdminLoginList | Indica a lista de SamAccountName de administradores únicos. **O valor é embaralhado.** | {AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(sempre embaralhado)** |
| TotalApiRequests | Indica as solicitações de API do serviço de Orquestração. | {TotalApiRequests: 1000} |
| BackupCount | Indica a contagem de backups operados pelo administrador do Studio. | {BackupCount: 200} |
| RestoreCount | Indica a contagem de restaurações que foram operadas pelo administrador do Studio. | {RestoreCount: 20} |

# Director

## Relatório de uso

### CABEÇALHOS

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| ver. | Indica a versão do evento de uso da licença. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | 8c2e20a5-ca3f-4401-ad69-d037933c40a0 |
| tipo | Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem. | Telemetry |
| st | Indica o carimbo de data/hora quando o evento é gerado no Studio. | 2024-03-22T01:32:23.4056195Z |
| Produção | Identifica o produto de origem e a implantação do evento de uso. | XenApp.Monitor |
| prodVer | Indica a versão do produto Director. | 7.42.0.0 |
| dvcName | Nome do servidor | C758LH671A44B3F7 |

### PAYLOAD

| CAMPO | DESCRIÇÃO | EXEMPLO | |
|---|---|---|---|
| AdminLoginCount | Esta é uma seção da carga útil que fornece a contagem de logins de administrador. | tipo: AdminLogin estatísticas<br><br>0: 1<br><br>1: 7 | |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| FeatureUsageCount | Esta seção do payload contém a contagem de recursos principais usados no Director. | tipo: FeatureUsage<br>estatísticas<br><br>0: 15<br><br>1: 20<br><br>5: 10 |
| OdataUsageCount | Esta seção do payload contém a contagem de uso da API Odata | tipo: OData_v3<br>estatísticas<br><br>0: 1<br><br>2: 7<br><br>5: 9<br><br>tipo: OData_v4<br><br>estatísticas<br><br>0: 1<br><br>2: 8<br><br>6: 7 |
| AppUsage | Indica as métricas de uso semanais dos aplicativos publicados. | tipo: AppUsage<br>cabeçalhos: applicationName,processName,totalDurationInMinutes<br><br>período: 01/05/24-07/05/24<br><br>valores: [<br><br>Calc_AWTSVDA-1907R,calc.exe,0.13, |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | | Notepad_AWTSVDA-1907R,notepad.exe,4] |
| UniqueAppUsers | Indica a contagem de usuários únicos juntamente com o total de inicializações de aplicativos em um mês para aplicativos publicados. | tipo: Usuários de Aplicativos Exclusivos<br>cabeçalhos: applicationName,totalLaunches,totalUniqueUsers<br>período: 04/24<br>valores: [<br>Calc_AWTSVDA-1907R,100,10,<br>Notepad_AWTSVDA-1907R,200,20] |
| DesktopUsage | Indica as métricas de uso semanais de desktops publicados. | tipo: Uso da Área de Trabalho<br>cabeçalhos: desktopGroupName,sessionSupport,totalDurationInMinutes<br>período: 01/05/24-07/05/24<br>valores: [<br>RdsDesktopAndAppGroup,1,10] |
| UniqueDesktopUsers | Indica a contagem de usuários únicos juntamente com o | tipo: UniqueDesktopUsers |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| | total de inicializações em um mês para desktops publicados. | cabeçalhos: desktopGroupName,totalLaunches,totalUniqueUsers<br><br>período: 04/24<br><br>valores: [<br><br>RdsDesktopAndAppGroup,10,5] |
| AvgLogonDuration | Indica a duração média do logon. | tipo: AvgLogonDuration<br>cabeçalhos: totalUserLogons, avgLogonDurationInSeconds<br><br>período: 01/05/24-07/05/24<br><br>valores: [<br><br>200,4] |
| CostSaved | Indica o custo economizado pelo cliente em um mês. | tipo: CustoEconomizado<br>cabeçalhos: hipervisor,custoEconomizado,moeda<br><br>período: 04/24<br><br>valores: [<br><br>1,221.02,1<br><br>2,301.02,2] |

## Administrador Delegado

### Uso

#### CABEÇALHOS

| CHAVE | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| versão | Indica a versão do evento de uso da licença. | 1 |
| id | Indica um identificador exclusivo do evento de uso. | 8c2e20a5-ca3f-4401-ad69-d037933c40a0 |
| tipo | Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem. | DelegatedAdmin.Usage |
| st | Indica o carimbo de data/hora quando o evento é gerado no Delegated Admin. | 2024-03-22T01:32:23.4056195Z |
| Produção | Identifica o produto de origem e a implantação do evento de uso. | XenDesktop.DelegatedAdmin (Cloud) |
| | | OnPrem.DelegatedAdmin (OnPrem) |
| prodVer | Indica a versão do produto Citrix DaaS ou Citrix Virtual Apps and Desktops. | 7.42.0.0 |

#### CARGA ÚTIL

| CHAVE | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| TotalCustomScopes | Indica o número total de escopos personalizados. | 2 |
| TotalCustomRoles | Indica o número total de funções personalizadas. | 4 |

### Embaralhar dados de telemetria de licenciamento

Considerando a sensibilidade das informações enviadas na telemetria de licença, a Citrix oferece uma opção para embaralhar os dados.

A tabela a seguir lista os dados que podem ser embaralhados:

| CAMPO | DESCRIÇÃO | EXEMPLO |
|---|---|---|
| usuário | Identifica o ID do Usuário para identificar de forma exclusiva um usuário que inicia o lançamento da sessão. | • fullName: `C648FE671A44B3F7`<br>• samName: `C758LH671A44B3F7`<br>• nome de usuário principal: `C7948FE671A44B3F7`<br>• userLicenseId: `C265FE671A44B3F7`<br>• userSid: `C097FE671A44B3F7` |
| dvc para dvcName | Indica o nome amigável para o dispositivo. | `C758LH671A44B3F7` |
| workerSid | Indica um identificador exclusivo para o VDA usado para a sessão. | `1E5LH671A44B3F7` |

| CAMPO | DESCRIÇÃO | EXEMPLO |
| --- | --- | --- |
| AdminLoginList | Indica a lista de administradores exclusivos SamAccountName | `{AdminLoginList: [UFMJ+JvXOTHO9mQD sOweiw= =]}` |

Para habilitar ou desabilitar a ofuscação, execute os seguintes comandos PowerShell no Delivery Controller.

> **Observação:**
>
> Para um cliente Citrix Service Provider™ (CSP), a ofuscação está sempre desabilitada. Clientes CSP não podem habilitar a ofuscação usando comandos PowerShell.

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando para habilitar ou desabilitar a ofuscação:

   Por padrão, o valor é `1`, ou `true`, o que habilita a ofuscação dos dados de telemetria de licença.

   Para desabilitar:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   Depois de desabilitar a ofuscação, você pode habilitá-la usando o seguinte comando:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

## Perguntas frequentes sobre licenciamento

> **Observação:**

- Para recursos de continuidade de negócios relacionados à pandemia de COVID-19, consulte CTX27055.
- Para informações gerais sobre como manter a continuidade dos negócios, consulte Business continuity — on demand.
- Para obter mais informações sobre o Citrix License Server atual, consulte Licensing.

## Licenciamento Citrix®

### Como posso obter meu arquivo de licença?

Enviamos o código de acesso da licença por e-mail. Existem três maneiras de gerar arquivos de licença usando o código de acesso da licença:

- O **Gerenciar Licenças** da sua página MyAccount em `citrix.com`. Para obter mais informações, consulte Manage licenses on citrix.com.
- Web Studio para alocar sua compra e o arquivo de licença é instalado automaticamente no seu Citrix License Server.
- Citrix Licensing Manager dentro do Citrix License Server para alocar sua compra e instalar seu arquivo de licença. Para obter mais informações, consulte Install icenses.

### Como alocar licença na minha conta?

Consulte Allocate licenses.

### Como adicionar licenças alocadas ao servidor de licenças?

Consulte Modify licenses.

### Quais portas TCP o licenciamento Citrix usa?

- O número da porta do Servidor de Licenças é 27000
- O número da porta do daemon do fornecedor é 7279
- A porta do Serviço Web para Licenciamento é 8083

### O que é o Citrix License Server?

O Citrix License Server é um sistema que permite que as licenças sejam compartilhadas pela rede. Para obter mais informações, consulte Visão geral das operações de licenciamento.

### Posso virtualizar ou agrupar o Citrix License Server?

Sim. Você pode virtualizar ou agrupar o Citrix License Server. Para obter mais informações, consulte Servidores de Licenças em Cluster.

### Quais benefícios estão disponíveis para mim se eu virtualizar o Citrix License Server?

A virtualização do Citrix License Server oferece uma solução redundante. Essa solução permite a mobilidade entre vários servidores físicos sem a necessidade de tempo de inatividade.

### Existem limitações a serem consideradas se eu virtualizar o Citrix License Server?

Não.

### O Citrix License Server gerencia todas as licenças para minha implantação do Citrix Virtual Apps and Desktops™?

O Citrix License Server gerencia todas as licenças que você recebe para o Citrix Virtual Apps™ e Desktop, exceto as licenças da Premium Edition usadas com o Citrix Gateway. Os servidores de licenças incorporados aos dispositivos de rede, conforme exigido para esses dispositivos de rede orientados à segurança, gerenciam essas licenças.

### O que é o Citrix Licensing Manager?

O Citrix Licensing Manager permite o download e a alocação de arquivos de licença do License Server no qual você instalou o Citrix Licensing Manager. O Citrix Licensing Manager é o método de gerenciamento de License Server recomendado, que permite o seguinte:

- Registro de código curto do Servidor de Licenças no Citrix Cloud™ e fácil remoção do registro.
- Configurar contas de usuário e grupo.
- Use o painel para exibir licenças instaladas, em uso, expiradas e disponíveis, e datas de Customer Success Services.
- Exportar dados de uso de licença para uso em relatórios.
- Configurar o período de retenção de dados de uso histórico. O período de retenção de dados padrão é de 180 dias.
- Instalação simplificada de arquivos de licença no Servidor de Licenças usando um código de acesso de licença ou arquivo baixado.
- Ativar e desativar o modo de intermitência de licença.
- Configurar o Programa de Melhoria da Experiência do Cliente (CEIP) e o Call Home.
- Verifica automaticamente ou manualmente as licenças de renovação dos Customer Success Services e notifica você ou instala as licenças, se encontradas.

- Notifica você sobre o estado do Servidor de Licenças - Licença de inicialização ausente, problemas de tempo, falhas de upload.
- Modificar estas portas:
  - Servidor de Licenças (padrão 27000)
  - Daemon do Fornecedor (padrão 7279)
  - Serviços Web para Licenciamento (padrão 8083)

Para obter mais informações, consulte Citrix Licensing Manager.

### Onde está o Citrix License Administration Console?

O License Administration Console não é mais compatível e foi removido do License Server versão 11.16.6. Recomendamos que você use o Citrix Licensing Manager.

Você pode usar o Studio para gerenciar e rastrear o licenciamento, desde que o License Server esteja no mesmo domínio que o Studio, ou em um domínio confiável.

Para obter mais informações, consulte Citrix Licensing Manager.

### Qual é o período de atribuição de licença?

O período de atribuição de licença é o termo pelo qual uma licença do Citrix Virtual Apps and Desktops é atribuída a um usuário ou dispositivo. O período de atribuição de licença padrão é de 90 dias.

### Como sei quantas licenças minha organização comprou?

Todas as licenças compradas estão disponíveis para revisão e acesso a qualquer momento (24 horas por dia, 7 dias por semana) na sua caixa de ferramentas segura **Gerenciar Licenças** na sua página **Minha Conta** em `<https://www.citrix.com>`.

### Como sei quantas licenças estão em uso a qualquer momento?

O Citrix Licensing Manager e o Studio fornecem detalhes sobre o uso da licença em tempo real.

### Recuperação de desastres e manutenção do License Server

Para obter informações sobre recuperação de desastres e manutenção do seu License Server, consulte Recuperação de desastres e manutenção na documentação de Licenciamento Citrix.

# Licenciamento do Citrix Virtual Apps and Desktops

## Como o Citrix Virtual Apps and Desktops é licenciado?

O licenciamento do Citrix Virtual Apps and Desktops oferece modelos de licença por usuário/dispositivo e concorrentes.

**Usuário/dispositivo:**

O modelo flexível de usuário/dispositivo se alinha com:

- Uso de desktop em toda a empresa.
- Licenciamento subjacente de virtualização de desktop da Microsoft.
- Licenciamento simultâneo para clientes com usuários que precisam de acesso apenas ocasional aos seus desktops e aplicativos virtuais.

O licenciamento de usuário/dispositivo oferece aos usuários acesso aos seus desktops e aplicativos virtuais a partir de um número ilimitado de dispositivos. As licenças de dispositivo oferecem a um número ilimitado de usuários acesso aos seus desktops e aplicativos virtuais a partir de um único dispositivo. Essa abordagem oferece máxima flexibilidade e melhora o alinhamento com o licenciamento de virtualização de desktop da Microsoft.

> **Importante:**

> Não é possível alocar licenças manualmente a um usuário ou dispositivo. O License Server ou o serviço de nuvem atribui as licenças. Com o licenciamento de usuário/dispositivo, uma vez que uma licença é atribuída, ela não pode ser atribuída a outro usuário até depois de 90 dias de inatividade.

> **Simultâneo:**

As licenças simultâneas permitem uma conexão a um número ilimitado de aplicativos e desktops virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida apenas durante uma sessão ativa. Se a sessão for desconectada ou encerrada, a licença é devolvida ao pool.

Para obter mais informações sobre o licenciamento de usuário/dispositivo, consulte Licença de usuário/dispositivo e licenças simultâneas, consulte Licença simultânea.

### É possível experimentar o Citrix Virtual Apps and Desktops antes de comprar licenças?

Sim. Você pode baixar o software Citrix Virtual Apps and Desktops e executá-lo no modo de avaliação. O modo de avaliação permite que você use o Citrix Virtual Apps and Desktops no local por 30 dias, para 10 conexões, sem uma licença. Para obter mais informações, consulte Licenças de avaliação.

O Citrix DaaS™ (anteriormente serviço Citrix Virtual Apps and Desktops) para Citrix Cloud está disponível para serviço de avaliação mediante aprovação. Verifique com seu representante Citrix para obter mais detalhes.

### Como a Citrix define a simultaneidade para o Citrix Virtual Apps and Desktops?

O modelo simultâneo do Citrix Virtual Apps and Desktops permite uma conexão a um número ilimitado de aplicativos e desktops virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida apenas durante uma sessão ativa. Se a sessão for desconectada ou encerrada, a licença é devolvida ao pool para reemissão. Para obter mais informações, consulte Licença simultânea.

### Posso implantar várias edições de licenças do Citrix Virtual Apps and Desktops em um License Server comum?

Sim. O License Server gerencia licenças para Citrix Virtual Apps e Desktops simultaneamente. Recomendamos que você instale a versão mais recente do License Server. Se você não tiver certeza se a versão do seu License Server está atualizada, verifique-a comparando sua versão com o número no site de downloads da Citrix.

### Um único site pode usar licenças do Citrix Virtual Apps e do Citrix Virtual Apps and Desktops?

Dependendo da versão, um único site do Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode suportar ambos os modelos de licenciamento - usuário/dispositivo ou simultâneo. Um único site do Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode suportar apenas uma edição. Para mais informações, consulte Licenciamento multi-tipo.

As versões mínimas que suportam licenciamento multi-tipo são XenApp e XenDesktop 7.15 Long Term Service Release (LTSR) e Citrix Virtual Apps and Desktops 7 1808.

### Posso selecionar Citrix Virtual Apps simultâneo como modelo de produto se eu tiver licenças de usuário/dispositivo do Citrix Virtual Apps and Desktops ou licenças simultâneas do Citrix Virtual Apps and Desktops instaladas no License Server?

Se você usa o Citrix Virtual Apps como um recurso do Citrix Virtual Apps and Desktops Advanced ou Premium Edition, o modelo de licença dele é o mesmo da sua edição Advanced ou Premium do

Citrix Virtual Apps and Desktops. Se você adquiriu o Citrix Virtual Apps and Desktops, configure seu licenciamento como Citrix Virtual Apps and Desktops, mesmo que planeje usar apenas a funcionalidade do Virtual Apps. Selecione Citrix Virtual Apps como um modelo de produto somente se você tiver licenças autônomas simultâneas deste produto instaladas no License Server.

**Quais componentes de produto estão incluídos em cada edição do Citrix Virtual Apps e do Citrix Virtual Apps and Desktops?**

Para uma matriz completa de recursos por edição, consulte Recursos do Citrix Virtual Apps and Desktops.

**Como faço para licenciar ambientes Citrix Virtual Desktops™ em conformidade com o EULA do Citrix Virtual Apps and Desktops?**

Para implantar o Citrix Virtual Apps and Desktops sob o modelo de licença de usuário/dispositivo ou simultâneo em conformidade com o EULA do Citrix Virtual Apps and Desktops, aplique os arquivos de licença ao seu License Server. O License Server então controla e monitora a conformidade da licença. Recomendamos que você configure seu produto com base no que você adquiriu. Por exemplo, se você adquirir o Citrix Virtual Apps and Desktops Premium, mas quiser usar apenas o recurso Citrix Virtual Apps, configure o produto para Citrix Virtual Apps and Desktops para atender à conformidade. Para mais informações, consulte o Centro de Conformidade de Licenças de Produto.

**Como faço para licenciar ambientes Citrix Virtual Apps em conformidade com o EULA do Citrix Virtual Apps?**

Para implantar o Citrix Virtual Apps sob o modelo de licença simultânea em conformidade com o EULA do Citrix Virtual Apps, aplique os arquivos de licença ao seu License Server. O License Server então controla e monitora a conformidade da licença.

**Existe um requisito de licenciamento para as Opções de Manutenção do Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) ou Current Release (CR)?**

As Opções de Manutenção do Citrix Virtual Apps and Desktops, como o Long-Term Service Release, são um benefício do programa Customer Success Services. Você deve ter Customer Success Services ativos para se qualificar para os benefícios do LTSR. Para mais informações, consulte [Opções de Manutenção do Citrix Virtual Apps, Citrix Virtual Apps and Desktops e XenServer.

### Como funcionam as horas agrupadas do serviço de isolamento de navegador remoto (RBI)?

Ao adquirir um mínimo de 25 usuários do serviço, você recebe 5000 horas de direitos para usar o serviço, agrupadas para todos os usuários. Compras subsequentes de direitos de usuário não aumentam o direito a horas agrupadas. Para aumentar o direito a horas de serviço, compre pacotes de complementos.

### Posso usar o Acesso Remoto ao PC com licenças CCU?

Sim.

Para obter informações sobre o Acesso Remoto ao PC, consulte Acesso Remoto ao PC.

### O que acontece quando a manutenção de software expira para o meu ambiente Citrix?

Quando sua Manutenção de Software (SWM) ou assinatura expira, o acesso a atualizações de software e suporte técnico é pausado. Além disso, dependendo do seu tipo de licença e versão do produto, usuários finais e administradores receberão notificações de aviso específicas indicando que o ambiente não é suportado.

Essas notificações são acionadas somente quando todas as licenças no servidor expiraram.

#### EXPERIÊNCIA DO USUÁRIO FINAL

Os usuários receberão uma mensagem de aviso após iniciar uma sessão. A mensagem indica:

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

#### EXPERIÊNCIA DO ADMINISTRADOR

Os administradores verão alertas de aviso no console do Citrix Studio, alertando-os sobre a expiração iminente ou ativa.

#### COMPORTAMENTO DE EXPIRAÇÃO POR TIPO DE LICENÇA

O momento dessas mensagens depende do tipo de licença e da versão do Citrix Virtual Apps and Desktops instalada.

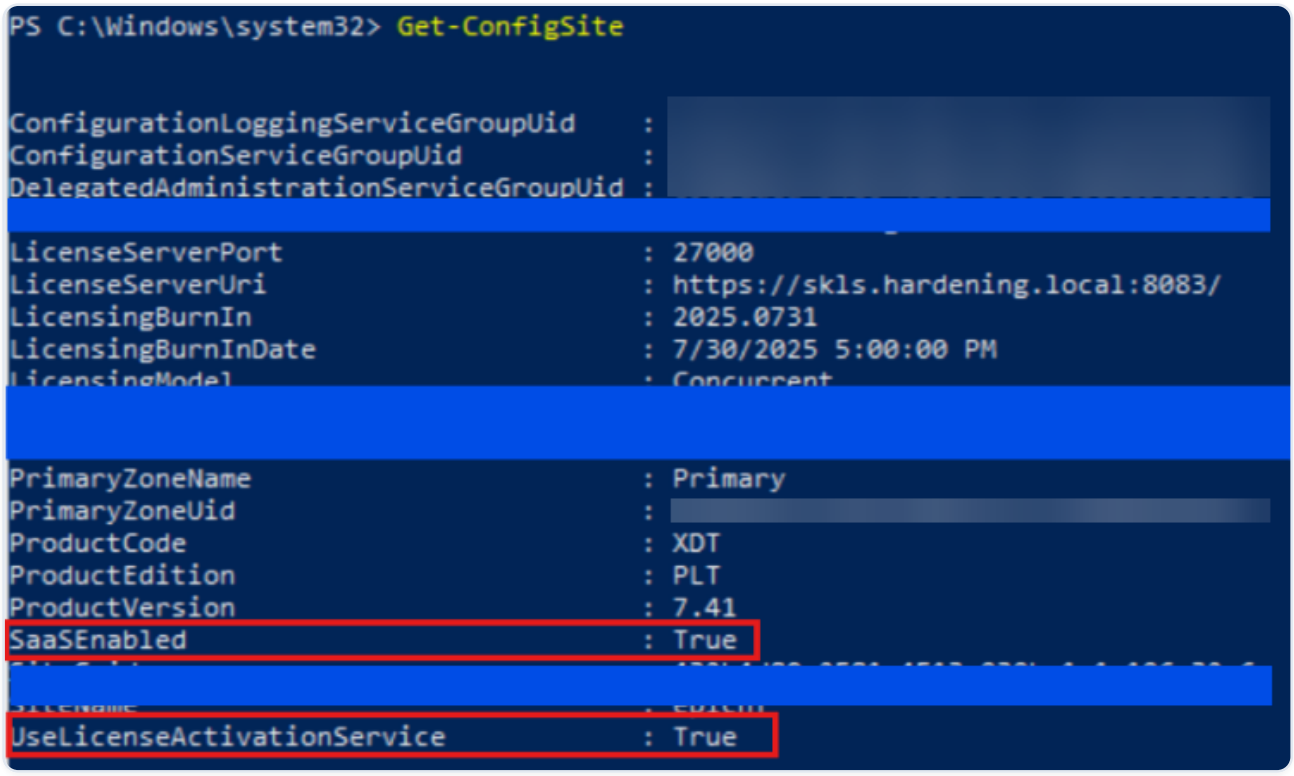
#### LICENÇAS DE ASSINATURA LOCAIS

- Aviso ao Usuário Final: Aparece após a expiração da assinatura, durante o período de carência.
- Aviso ao Administrador: Aparece no Studio 30 dias antes da expiração da assinatura.

- Versões Suportadas:
  - Versão Atual: Citrix Virtual Apps and Desktops 2411 e superior.
  - LTSR: 2203 CU6, e 2402 CU1 e versões LTSR posteriores

### Como posso verificar o estado LAS de um site?

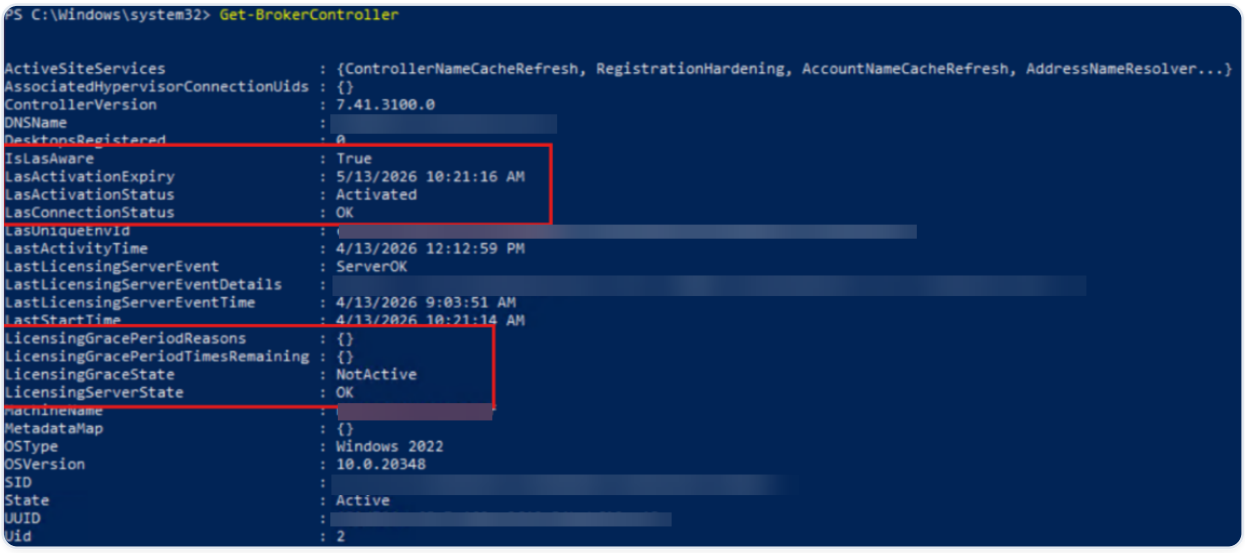
Execute `Get-configsite` para verificar o estado de ativação do LAS e o status do bit SaaS.



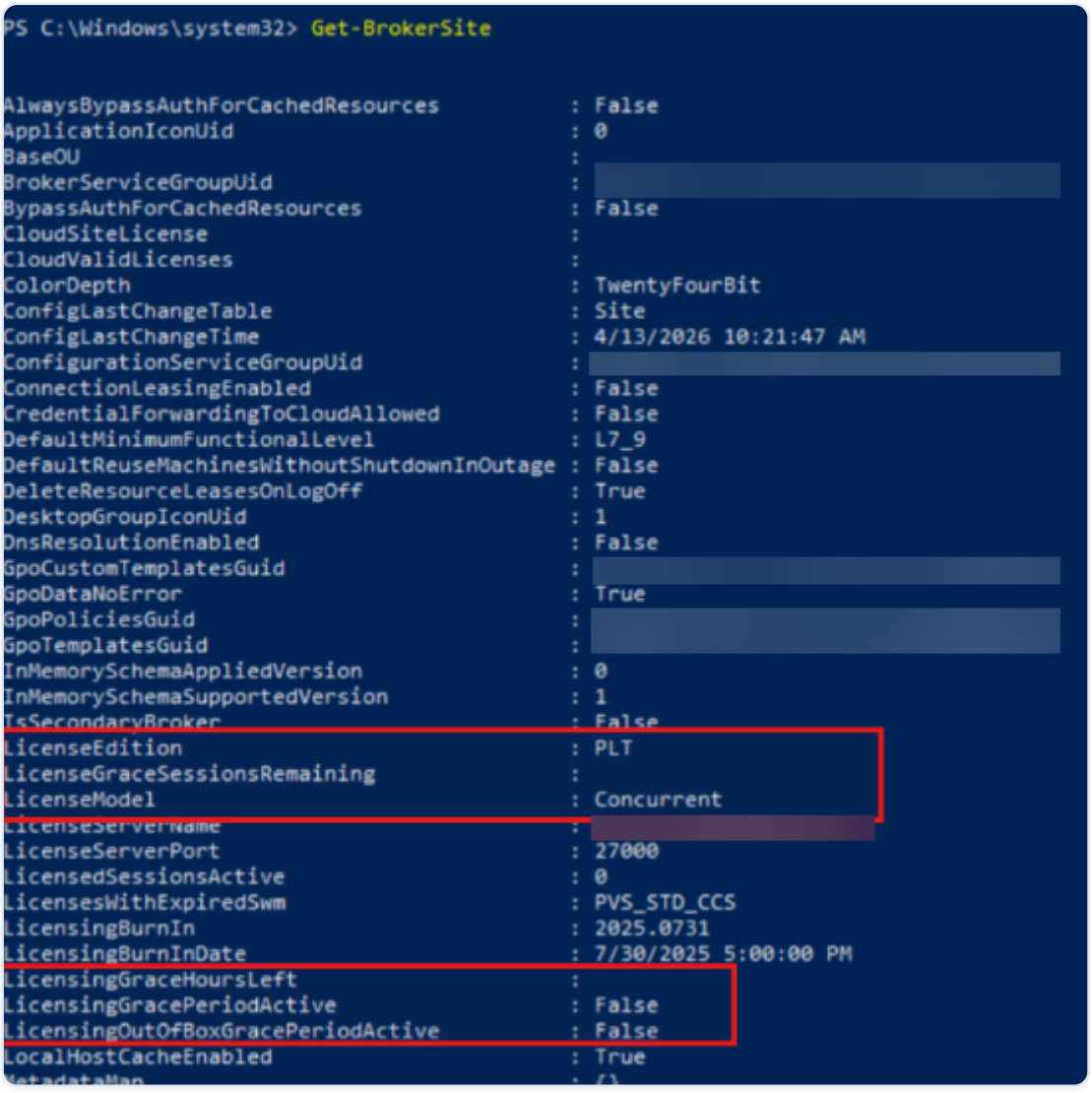

### Como posso verificar se um site está no modo de cache de licença de emergência?

Execute `Get-Brokercontroller` e `Get-brokersite` para obter detalhes sobre o modo de cache de emergência e o tempo restante.

- Saída de `Get-Brokercontroller`:




- Saída de `Get-brokersite`:




Para informações detalhadas sobre os comandos, consulte:

- Get-BrokerController

- Get-ConfigSite

Para obter informações sobre os logs do visualizador de eventos do Delivery Controller relacionados ao licenciamento, consulte Logs do visualizador de eventos relacionados a eventos de licenciamento.

## Licenças de usuário ou dispositivo

### Como a Citrix aloca licenças para usuários no modelo de licenciamento de usuário/dispositivo?

Com o modelo de licença de usuário/dispositivo, o License Server atribui a licença a um ID de usuário exclusivo. Ele permite que esse único usuário tenha conexões ilimitadas de dispositivos ilimitados. Se um usuário se conecta a um desktop ou dispositivo, o usuário requer uma licença atribuída a ele para acessar um desktop ou aplicativo virtual. O License Server ou o serviço de nuvem atribui a licença. Você não pode atribuir essas licenças manualmente. A licença é atribuída ao usuário, não ao dispositivo compartilhado. Uma vez atribuída, a licença não pode ser atribuída a outro usuário até depois de 90 dias de inatividade. Para obter mais informações, consulte Licença de usuário/dispositivo.

### Como a Citrix define um dispositivo licenciado no modelo de licenciamento de usuário/dispositivo?

Um dispositivo licenciado requer um ID de dispositivo de endpoint exclusivo. No modelo de usuário/dispositivo, um dispositivo é qualquer equipamento que você autorizou para uso por qualquer indivíduo para acessar instâncias do Citrix Virtual Apps and Desktops. Para um dispositivo compartilhado, uma única licença de usuário/dispositivo do Citrix Virtual Apps and Desktops pode suportar vários usuários que compartilham o dispositivo. Por exemplo, um dispositivo compartilhado pode ser uma estação de trabalho de sala de aula ou uma estação de trabalho clínica em um hospital.

### Posso converter minhas licenças concorrentes do Citrix Virtual Desktops Standard Edition para o modelo de usuário/dispositivo?

Você não pode converter licenças concorrentes do Citrix Virtual Desktops Standard Edition em licenças de usuário/dispositivo do Citrix Virtual Desktops Standard Edition. Da mesma forma, você não pode converter licenças de usuário/dispositivo do Citrix Virtual Desktops Standard Edition em licenças concorrentes do Citrix Virtual Desktops Standard Edition.

Se você tiver licenças concorrentes do Citrix Virtual Desktops Standard Edition e quiser o modelo de licença de usuário/dispositivo, atualize para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.

| DE | PARA CONCORRENTE PADRÃO | PARA USUÁRIO/ DISPOSITIVO PADRÃO | PARA USUÁRIO/ DISPOSITIVO AVANÇADO | PARA USUÁRIO/ DISPOSITIVO PREMIUM |
|---|---|---|---|---|
| Licenças simultâneas do Citrix Virtual Desktops Standard Edition | N/A | Conversão de simultâneo para usuário/ dispositivo NÃO permitida | Você não pode converter modelos de licença, mas pode fazer upgrade para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition. | Você não pode converter modelos de licença, mas pode fazer upgrade para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition. |
| Licenças de usuário/ dispositivo do Citrix Virtual Desktops Standard Edition | Conversão de usuário/ dispositivo para simultâneo NÃO permitida | N/A | N/A | N/A |

**Como o licenciamento simultâneo funciona de forma diferente do licenciamento por usuário/dispositivo?**

Baseamos o licenciamento simultâneo em conexões de dispositivos simultâneas. Uma licença simultânea está em uso apenas quando um dispositivo estabeleceu uma conexão ativa. Assim que a conexão termina, a licença simultânea retorna ao pool de licenças para uso imediato. Recomendamos este modelo de licenciamento para uso ocasional. As licenças de usuário/ dispositivo são alugadas por um período e não estão disponíveis para outros usuários até que o aluguel expire.

**No modelo de usuário/dispositivo, podemos alocar licenças para usuários e dispositivos na mesma empresa?**

Sim. Ambos os tipos podem estar presentes na mesma empresa. O License Server atribui licenças de forma otimizada a usuários ou dispositivos com base no uso. Você não pode atribuir essas licenças manualmente.

### Como decido quantos usuários ou dispositivos licenciar?

Avalie os requisitos do caso de uso para determinar o número apropriado de licenças. O licenciamento por usuário/dispositivo permite acesso ilimitado a desktops virtuais e aplicativos virtuais ilimitados a partir de um número ilimitado de dispositivos. O licenciamento simultâneo permite acesso ilimitado a desktops virtuais e aplicativos virtuais ilimitados a partir de um único dispositivo que um número ilimitado de usuários pode usar. Considere a seguinte fórmula:

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

### No modelo de usuário/dispositivo, qual é o número máximo de dispositivos que um usuário licenciado pode usar para se conectar ao meu ambiente?

Cada usuário licenciado tem o direito de usar um número ilimitado de dispositivos conectados ou offline.

### Sob o modelo de usuário/dispositivo, qual é o número máximo de usuários que podem acessar um dispositivo licenciado?

Cada dispositivo licenciado pode atender a um número ilimitado de usuários dentro de uma organização.

### Sob o modelo de usuário/dispositivo, qual é o número máximo de desktops virtuais ou aplicativos web RBI que um usuário licenciado pode consumir a qualquer momento?

Cada usuário licenciado pode se conectar a um número ilimitado de desktops virtuais ou aplicativos web.

**Posso adquirir licenças do Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados no meu ambiente Citrix Virtual Apps and Desktops existente?**

Sim. Você pode adquirir licenças do Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados no seu ambiente Citrix Virtual Apps and Desktops existente.

**Como faço para liberar uma licença de usuário/dispositivo autorizado?**

Para liberar a atribuição de um usuário/dispositivo autorizado, use o utilitário `udadmin` de acordo com os termos do EULA. O Servidor de Licenças então atribui a licença ao próximo usuário/dispositivo apropriado. Para mais informações, consulte Exibir ou liberar licenças para usuários ou dispositivos.

**O que acontece se eu exceder minha contagem de licenças de usuário/dispositivo adquiridas?**

As licenças de usuário/dispositivo incluem um limite de 10% de excedente (overdraft), que é incluído quando as licenças são geradas. O excedente também é incluído na contagem de licenças instaladas. Se o pico de uso exceder a contagem instalada, incluindo o excedente, o acesso para mais usuários será negado. Adquira e implante uma nova licença para permitir o acesso a mais usuários.

Se todas as licenças estiverem em uso, incluindo o excedente de licenças, o modo de burst de licença permite conexões ilimitadas a um produto. O modo de burst de licença lhe dá tempo para determinar por que você excedeu a contagem máxima de licenças e para adquirir mais licenças sem interromper seus usuários. Este período dura até que 15 dias se passem ou você instale mais licenças de varejo, o que ocorrer primeiro. Para mais informações, consulte Modo de burst de licença.

O Director exibe os estados do modo de cache de licenças. Para mais informações, consulte Painéis no Painel do Director.

**Qual é o número máximo de aplicativos virtuais que um usuário licenciado pode consumir a qualquer momento?**

Cada usuário licenciado pode se conectar a um número ilimitado de aplicativos virtuais.

**O que acontece se um usuário licenciado sair da minha organização?**

Quando um usuário licenciado existente deixa sua organização, você pode liberar a licença do usuário que está saindo sem notificar a Citrix. Use o utilitário `udadmin` para liberar a licença. Se você não liberar a licença, o Servidor de Licenças libera automaticamente qualquer licença após 90 dias de inatividade. Esta informação está sujeita aos termos especificados no EULA.

**O que acontece se um usuário licenciado estiver ausente por um período prolongado?**

Se um usuário licenciado existente estiver ausente por um período prolongado, você pode liberar a licença sem notificar a Citrix, para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

**O que acontece se substituirmos um dispositivo licenciado em minha organização?**

Se você substituir um dispositivo licenciado existente, poderá liberar a licença sem notificar a Citrix para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

**O que acontece se um dispositivo licenciado estiver fora de serviço por um período prolongado?**

Quando um dispositivo licenciado existente estiver fora de serviço por um período prolongado, você pode liberar a licença sem notificar a Citrix, para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar as licenças. Se você não liberar a licença, o Servidor de Licenças libera automaticamente qualquer licença após 90 dias de inatividade. Esta informação está sujeita aos termos especificados no EULA.

**Posso alternar licenças de usuário para licenças de dispositivo e vice-versa depois de atribuir as licenças a um dispositivo ou usuário?**

Sim. Essa alteração acontece automaticamente. O Servidor de Licenças atribui licenças a usuários ou dispositivos com base nos padrões de uso. Se os padrões de uso mudarem, o Servidor de Licenças pode alternar a atribuição com base no novo uso. O Servidor de Licenças sempre atribui licenças da forma mais econômica para o cliente. Além disso, o Servidor de Licenças monitora as licenças para identificar licenças **não utilizadas** após o período de atribuição de 90 dias. Você pode reatribuir licenças identificadas como não utilizadas após o período de atribuição de 90 dias para outros usuários ou dispositivos.

## Licenças simultâneas

**No modelo simultâneo, qual é o número máximo de desktops virtuais que um usuário licenciado do Citrix Virtual Apps and Desktops pode consumir a qualquer momento?**

Um endpoint pode atender a muitos usuários e permite conexões ilimitadas.

**Posso implantar licenças simultâneas de uma versão anterior do Citrix Virtual Apps and Desktops e novas licenças de usuário/dispositivo ou simultâneas em um único Servidor de Licenças?**

Sim. Você pode continuar a usar o mesmo Servidor de Licenças para oferecer suporte a implantações licenciadas por usuário/dispositivo ou simultâneas.

### Posso implantar licenças simultâneas e licenças de usuário/dispositivo ou simultâneas em um único Servidor de Licenças?

Sim. Você pode continuar a usar o mesmo Servidor de Licenças para suportar implantações licenciadas simultâneas e por usuário/dispositivo ou simultâneas.

### As edições Advanced e Premium do Citrix Virtual Apps and Desktops incluem licenças simultâneas do Citrix Virtual Apps?

As licenças de usuário/dispositivo Advanced e Premium do Citrix Virtual Apps and Desktops incluem licenças simultâneas do Citrix Virtual Apps apenas para compatibilidade. Essas licenças simultâneas são para uso apenas com versões anteriores do produto que são incompatíveis com licenças de usuário/dispositivo. O uso das licenças de compatibilidade simultâneas incluídas com as licenças de usuário/dispositivo é permitido apenas com estas versões - versões do XenApp anteriores a 6.5 e versões do XenDesktop anteriores ao Service Pack 1 da versão 5.0.

### O que acontece se eu exceder minha contagem de licenças simultâneas compradas?

Se todas as licenças estiverem em uso, o modo de intermitência de licença permite conexões ilimitadas a um produto. O modo de intermitência de licença lhe dá tempo para determinar por que você excedeu a contagem máxima de licenças e para comprar mais licenças sem interromper seus usuários. Este período dura até que 15 dias se passem ou você instale mais licenças de varejo, o que ocorrer primeiro. Para obter mais informações, consulte Modo de intermitência de licença.

O Director exibe os estados do modo de cache de licença. Para obter mais informações, consulte Painéis no Painel do Director.

## Licenças de estouro

### Como obtenho licenças de estouro?

Produtos (excluindo Citrix Cloud) que suportam modelos de licença por usuário/dispositivo, por usuário ou por dispositivo incluem um recurso de estouro de licença que permite usar um número limitado de licenças extras para evitar a negação de acesso. Oferecemos qualquer recurso de estouro como uma conveniência, não como um direito de licença. Licenças simultâneas e de servidor não contêm estouro. Quaisquer licenças de estouro usadas devem ser compradas dentro de 30 dias do primeiro uso, mas o uso não é limitado a 30 dias. A Citrix reserva-se o direito de remover qualquer recurso de estouro em novos lançamentos de produtos. Para obter mais informações, consulte Estouro de licença.

**Como posso identificar um estouro de licença?**

Você pode visualizar informações de uso, incluindo o número de licenças em estouro no Citrix Licensing Manager. O Studio também contém informações de uso de estouro.

**O que acontece quando uma licença de estouro é consumida?**

Uma licença é atribuída das suas licenças instaladas para permitir o acesso ao seu ambiente Citrix Virtual Apps and Desktops. Esta licença de estouro fornece tanto acesso e funcionalidade quanto as suas outras licenças.

**Posso receber um alerta quando minhas licenças de estouro forem consumidas?**

Atualmente, não há alertas específicos fornecidos quando as licenças de estouro são consumidas.

**Por quanto tempo uma licença de overdraft pode ser consumida?**

Adquira quaisquer licenças de overdraft usadas dentro de 30 dias do primeiro uso.

### Outras informações de licenciamento específicas do produto

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer
- Citrix Licensing

# Balancear carga de máquinas

> **Observação:**

> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este recurso está disponível apenas no Web Studio.

> Este recurso se aplica a todos os seus catálogos — catálogos de SO de sessão única ou de SO de múltiplas sessões. O balanceamento de carga vertical se aplica apenas a máquinas de SO de múltiplas sessões.

> O balanceamento de carga pode ser configurado no nível do site e no nível do grupo de entrega. Você tem duas opções: vertical e horizontal. Por padrão, o balanceamento de carga horizontal está ativado.

## Configurações de balanceamento de carga no nível do site

- **Balanceamento de carga vertical**. Atribui uma sessão de usuário de entrada à máquina mais carregada que ainda não atingiu a carga máxima. Isso satura as máquinas existentes antes de passar para novas máquinas. Usuários que se desconectam das máquinas existentes liberam capacidade nessas máquinas. As cargas de entrada são então atribuídas a essas máquinas. O balanceamento de carga vertical degrada a experiência do usuário, mas reduz os custos (as sessões maximizam a capacidade da máquina ligada).

  Exemplo: Você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com as primeiras 10 sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

  > **Dica:**
  >
  > Para especificar o número máximo de sessões que uma máquina pode hospedar, use a configuração de política Número máximo de sessões.
  >
  > Alternativamente, você pode usar o PowerShell para habilitar ou desabilitar o balanceamento de carga vertical em todo o site. Use a configuração `UseVerticalScalingForRdsLaunches` no cmdlet `Set-BrokerSite`. Use `Get-BrokerSite` para exibir o valor da configuração `UseVerticalScalingForRdsLaunches`. Consulte a ajuda do cmdlet para obter detalhes.

- **Balanceamento de carga horizontal**. Atribui uma sessão de usuário de entrada à máquina ligada menos carregada disponível. O balanceamento de carga horizontal melhora a experiência do usuário, mas aumenta os custos (porque mais máquinas são mantidas ligadas). Por padrão, o balanceamento de carga horizontal está ativado.

  Exemplo: Você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com cinco sessões simultâneas. A segunda máquina também lida com cinco.

Para configurar este recurso, no Web Studio, selecione **Configurações** no painel esquerdo. Selecione uma opção em **Balancear carga de catálogos de múltiplas sessões**.

### Configurações de balanceamento de carga no nível do grupo de entrega

A configuração do balanceamento de carga no nível do grupo de entrega permite substituir as configurações de balanceamento de carga herdadas do nível do site. Você pode atingir a utilização máxima para cada máquina ao selecionar o balanceamento de carga vertical no nível do grupo de entrega. Isso ajudará a reduzir custos em nuvens públicas. Esta configuração pode ser feita durante a criação de um novo grupo de entrega ou edição de um grupo de entrega existente.

**Balanceamento de carga horizontal**. As sessões são distribuídas entre as máquinas ligadas. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina lida com cinco sessões simultâneas e a segunda máquina também lida com cinco.

**Balanceamento de carga vertical**. As sessões maximizam a capacidade da máquina ligada e economizam custos de máquina. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina lida com as primeiras 10 sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

## Cache de Host Local

Para garantir que o banco de dados do site Citrix Virtual Apps and Desktops esteja sempre disponível, a Citrix recomenda começar com uma implantação de SQL Server tolerante a falhas, seguindo as melhores práticas de alta disponibilidade da Microsoft. (Para recursos de alta disponibilidade do SQL Server suportados, consulte Bancos de Dados.) No entanto, problemas e interrupções de rede podem resultar na impossibilidade de os usuários se conectarem aos seus aplicativos ou desktops.

O recurso Cache de Host Local permite que as operações de intermediação de conexão em um site continuem quando ocorre uma interrupção. Uma interrupção ocorre quando a conexão entre um Delivery Controller™ e o banco de dados do site falha em um ambiente Citrix® local. O Cache de Host Local é ativado quando o banco de dados do site fica inacessível por 90 segundos.

A partir do XenApp e XenDesktop 7.16, o recurso de leasing de conexão (um recurso de alta disponibilidade predecessor em versões anteriores) foi removido do produto e não está mais disponível.

### Conteúdo dos dados

O Cache de Host Local inclui as seguintes informações, que é um subconjunto das informações no banco de dados principal:

- Identidades de usuários e grupos que têm direitos atribuídos a recursos publicados do site.

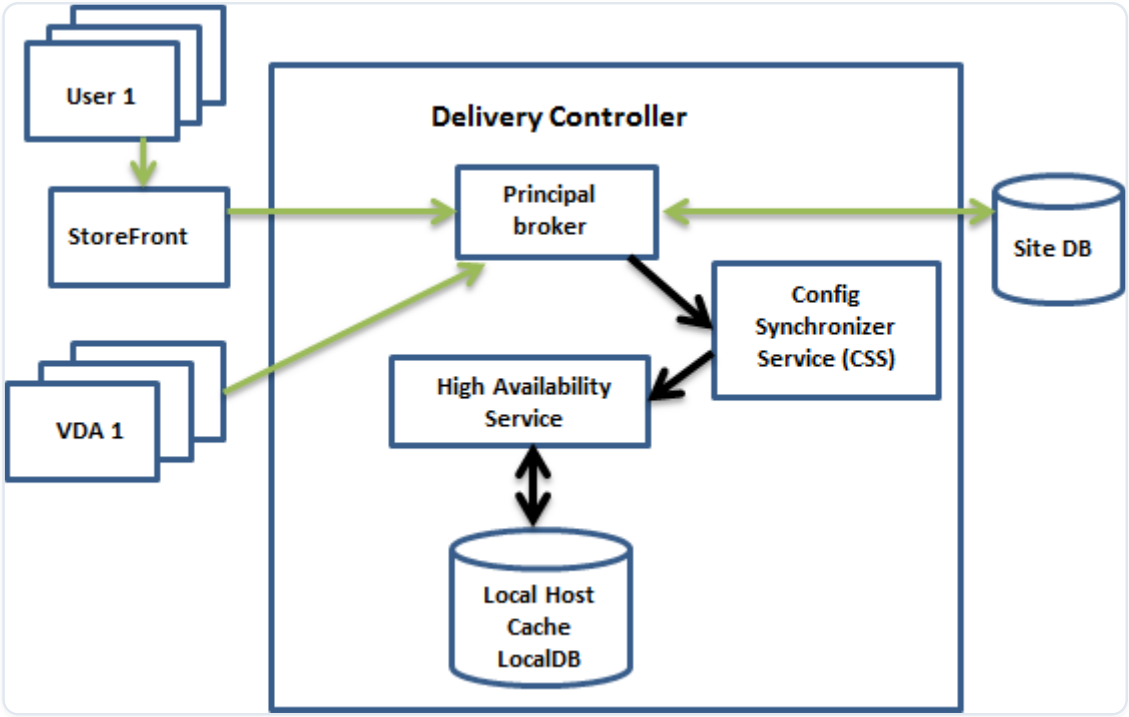
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados do site.
- Identidades de máquinas VDA (incluindo máquinas de Acesso Remoto para PC) configuradas no site.
- Identidades (nomes e endereços IP) de máquinas cliente Citrix Receiver™ sendo ativamente usadas para se conectar a recursos publicados.

Ele também contém informações para conexões atualmente ativas que foram estabelecidas enquanto o banco de dados principal estava indisponível:

- Resultados de qualquer análise de endpoint de máquina cliente realizada pelo Citrix Receiver.
- Identidades de máquinas de infraestrutura (como servidores NetScaler Gateway e StoreFront™) envolvidas com o site.
- Datas, horários e tipos de atividade recente dos usuários.

## Como funciona

O gráfico a seguir ilustra os componentes do Local Host Cache e os caminhos de comunicação durante as operações normais.



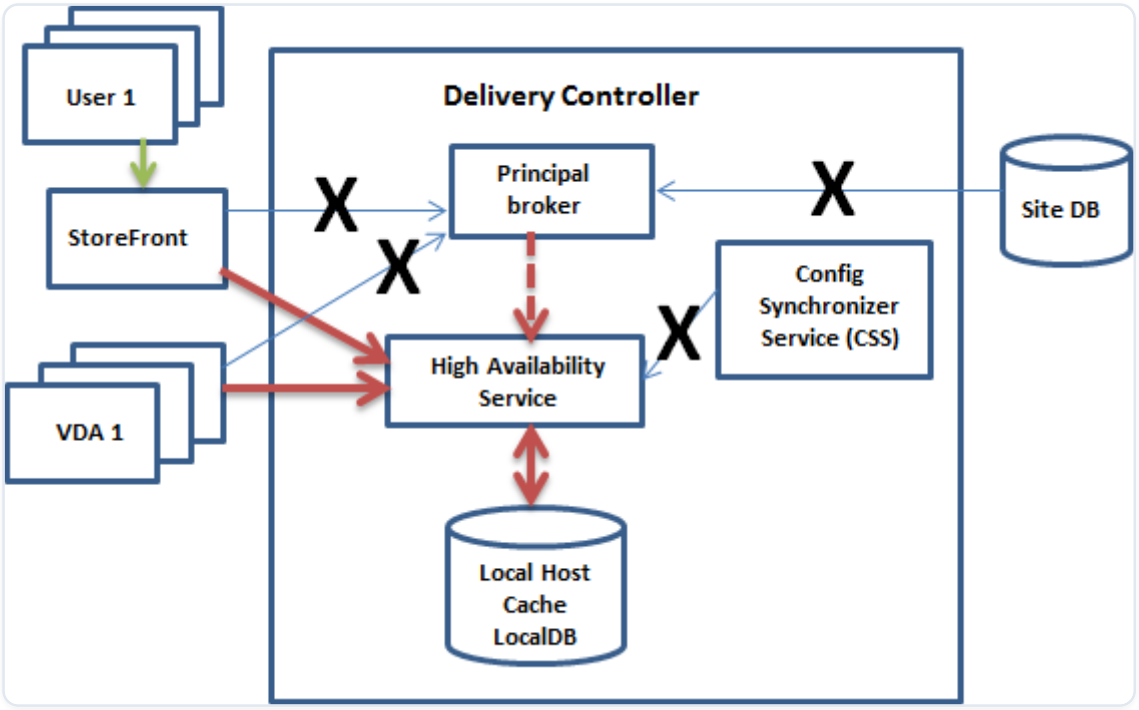
### Durante operações normais

- O *broker principal* (Citrix Broker Service) em um Controller aceita solicitações de conexão do StoreFront. O broker se comunica com o banco de dados do site para conectar usuários a VDAs que estão registrados no Controller.
- O Citrix Config Synchronizer Service (CSS) verifica com o broker aproximadamente a cada 5 minutos para ver se alguma alteração foi feita. Essas alterações podem ser iniciadas pelo administrador (como a alteração de uma propriedade de grupo de entrega) ou ações do sistema (como atribuições de máquina).
- Se uma alteração de configuração ocorreu desde a verificação anterior, o CSS sincroniza (copia) informações para um broker secundário no Controller. (O broker secundário também é conhecido como Serviço de Alta Disponibilidade.)

  Todos os dados de configuração são copiados, não apenas os itens que foram alterados desde a verificação anterior. O CSS importa os dados de configuração para um banco de dados Microsoft SQL Server Express LocalDB no Controller. Este banco de dados é referido como o banco de dados Local Host Cache. O CSS garante que as informações no banco de dados Local Host Cache correspondam às informações no banco de dados do site. O banco de dados Local Host Cache é recriado cada vez que a sincronização ocorre.

  O Microsoft SQL Server Express LocalDB (usado pelo banco de dados Local Host Cache) é instalado automaticamente quando você instala um Controller. (Você pode proibir esta instalação ao instalar um Controller a partir da linha de comando.) O banco de dados Local Host Cache não pode ser compartilhado entre Controllers. Você não precisa fazer backup do banco de dados Local Host Cache. Ele é recriado toda vez que uma alteração de configuração é detectada.
- Se nenhuma alteração ocorreu desde a última verificação, nenhum dado é copiado.

A imagem a seguir ilustra as alterações nos caminhos de comunicação se o broker principal perder contato com o banco de dados do site (uma interrupção começa).




### Durante uma interrupção

Quando uma interrupção começa:

- O broker secundário começa a ouvir e processar solicitações de conexão.
- Quando a interrupção começa, o broker secundário não possui dados de registro VDA atuais, mas quando um VDA se comunica com ele, um processo de registro é acionado. Durante esse processo, o broker secundário também obtém informações de sessão atuais sobre esse VDA.
- Enquanto o broker secundário está lidando com as conexões, o Brokering Principal continua a monitorar a conexão. Quando a conexão é restaurada, o Brokering Principal instrui o broker secundário a parar de escutar informações de conexão, e o Brokering Principal retoma as operações de corretagem. Na próxima vez que um VDA se comunicar com o Brokering Principal, um processo de registro é acionado. O broker secundário remove quaisquer registros VDA restantes da interrupção anterior. O CSS retoma a sincronização de informações quando descobre que ocorreram alterações de configuração na implantação.

No improvável evento de uma interrupção começar durante uma sincronização, a importação atual é descartada e a última configuração conhecida é usada.

O log de eventos fornece informações sobre sincronizações e interrupções.

Não há limite de tempo imposto para operação no modo de interrupção.

A transição entre o modo normal e o modo de interrupção não afeta as sessões existentes. Ela afeta apenas o lançamento de novas sessões.

Você também pode acionar intencionalmente uma interrupção. Consulte Forçar uma interrupção para obter detalhes sobre o porquê e como fazer isso.

### Sites com vários Controllers

Entre suas outras tarefas, o CSS fornece rotineiramente ao broker secundário informações sobre todos os Controllers na zona. (Se sua implantação não contiver várias zonas, esta ação afeta todos os Controllers no site.) Com essas informações, cada broker secundário sabe sobre todos os brokers secundários pares em execução em outros Controllers na zona.

Os brokers secundários se comunicam entre si em um canal separado. Esses brokers usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual broker secundário será responsável pelas operações de broker na zona se ocorrer uma interrupção. Durante a interrupção, todos os VDAs se registram no broker secundário eleito. Os brokers secundários não eleitos na zona rejeitam ativamente as solicitações de conexão de entrada e de registro de VDA.

Se um broker secundário eleito falhar durante uma interrupção, outro broker secundário será eleito para assumir, e os VDAs se registrarão no broker secundário recém-eleito.

Durante uma interrupção, se um Controller for reiniciado:

- Se esse Controller não for o broker eleito, a reinicialização não terá impacto.
- Se esse Controller for o broker eleito, um Controller diferente será eleito, fazendo com que os VDAs se registrem. Depois que o Controller reiniciado é ligado, ele assume automaticamente a função de broker, o que faz com que os VDAs se registrem novamente. Nesse cenário, o desempenho pode ser afetado durante os registros.

Se você desligar um Controller durante as operações normais e depois ligá-lo durante uma interrupção, o Local Host Cache não poderá ser usado nesse Controller se ele for eleito como o broker.

Os logs de eventos fornecem informações sobre as eleições.

## O que está indisponível durante uma interrupção e outras diferenças

Não há limite de tempo imposto para operar no modo de interrupção. No entanto, a Citrix recomenda restaurar a conectividade o mais rápido possível.

Durante uma interrupção:

- Você não pode usar o Studio.

- Você tem acesso limitado ao PowerShell SDK.
  - Você deve primeiro:
    - Adicione uma chave de registro `EnableCssTestMode` com o valor 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    - Use a porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - Após executar esses comandos, você pode acessar:
    - Todos os cmdlets `Get-Broker*`.
- As credenciais do hipervisor não podem ser obtidas do Serviço de Host. Todas as máquinas estão em estado de energia desconhecido e nenhuma operação de energia pode ser emitida. No entanto, as VMs no host que estão ligadas podem ser usadas para solicitações de conexão.
- Uma máquina atribuída pode ser usada somente se a atribuição ocorreu durante operações normais. Novas atribuições não podem ser feitas durante uma interrupção.
- O registro e a configuração automáticos de máquinas de Acesso Remoto a PC não são possíveis. No entanto, as máquinas que foram registradas e configuradas durante a operação normal são utilizáveis.
- Aplicativos hospedados em servidor e usuários de desktop podem usar mais sessões do que seus limites de sessão configurados, se os recursos estiverem em zonas diferentes.
- Os usuários podem iniciar aplicativos e desktops apenas a partir de VDAs registrados na zona que contém o broker secundário atualmente ativo/eleito. Lançamentos entre zonas (de um broker secundário em uma zona para um VDA em uma zona diferente) não são suportados durante uma interrupção.
- Se ocorrer uma interrupção do banco de dados do site antes do início de um reinício agendado para VDAs em um grupo de entrega, os reinícios começarão quando a interrupção terminar. Isso pode ter resultados não intencionais. Para obter mais informações, consulte Reinícios agendados atrasados devido a interrupção do banco de dados.
- Preferência de zona não pode ser configurada. Se configurada, as preferências não são consideradas para o lançamento da sessão.
- Restrições de tag, onde as tags são usadas para designar zonas, não são suportadas para lançamentos de sessão. Quando tais restrições de tag são configuradas e a opção verificação

avançada de integridade de uma loja StoreFront está habilitada, as sessões podem falhar intermitentemente ao iniciar.

## Suporte a aplicativos e desktops

O Cache de Host Local suporta aplicativos e desktops hospedados em servidor, e desktops estáticos (atribuídos).

O Cache de Host Local suporta VDAs de desktop em grupos de entrega agrupados, da seguinte forma:

- Por padrão, VDAs de desktop gerenciados por energia em grupos de entrega agrupados (criados por MCS ou Citrix Provisioning™) que têm a propriedade `ShutdownDesktopsAfterUse` habilitada não estão disponíveis para novas conexões durante um evento de Cache de Host Local. Você pode alterar esse padrão para permitir que esses desktops sejam usados durante o Cache de Host Local.

  No entanto, você não pode depender do gerenciamento de energia durante a interrupção. (O gerenciamento de energia é retomado após o retorno das operações normais.) Além disso, esses desktops podem conter dados do usuário anterior, pois não foram reiniciados.
- Para substituir o comportamento padrão, ele deve ser ativado em todo o site e para cada grupo de entrega afetado. Execute os seguintes cmdlets do PowerShell.

  Em todo o site:

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  Para cada grupo de entrega afetado, execute o seguinte comando PowerShell:

  ```
  Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
  ```

Para habilitar a configuração do grupo de entrega por padrão, execute o seguinte comando PowerShell:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Esta configuração se aplica a todos os novos grupos de entrega que são criados após a ativação desta configuração.

Para habilitar essa configuração para os grupos de entrega existentes, execute o seguinte comando PowerShell:

```
Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
```

Habilitar esse recurso no site e nos grupos de entrega não afeta como a propriedade `ShutdownDesktopsAfterUse` configurada funciona durante as operações normais. Quando esse recurso está habilitado, os VDAs não reinicializam automaticamente após a conclusão do evento LHC. VDAs de desktop gerenciados por energia em grupos de entrega agrupados podem reter dados de sessões anteriores até que o VDA seja reinicializado. Isso pode ocorrer quando um usuário faz logoff do VDA durante operações não-LHC ou a reinicialização pode ser acionada manualmente.

> **Importante:**
>
> Sem habilitar ReuseMachinesWithoutShutdownInOutageAllowed no nível do Site e ReuseMachinesWithoutShutdownInOutage no nível do grupo de entrega, todas as tentativas de iniciar sessões para VDAs de desktop gerenciados por energia em grupos de entrega agrupados falharão durante um evento de Cache de Host Local.

### Considerações sobre o tamanho da RAM

O serviço LocalDB pode usar aproximadamente 1,2 GB de RAM (até 1 GB para o cache do banco de dados, mais 200 MB para executar o SQL Server Express LocalDB). O broker secundário pode usar até 1 GB de RAM se uma interrupção durar um intervalo estendido com muitos logons ocorrendo (por exemplo, 12 horas com 10 mil usuários). Esses requisitos de memória são adicionais aos requisitos normais de RAM para o Controller, então você pode precisar aumentar a quantidade total de capacidade de RAM.

Se você usar uma instalação do SQL Server Express para o banco de dados do site, o servidor terá dois processos sqlserver.exe.

### Considerações sobre a configuração de núcleos de CPU e soquetes

A configuração da CPU de um Controller, particularmente o número de núcleos disponíveis para o SQL Server Express LocalDB, afeta diretamente o desempenho do Cache de Host Local, ainda mais do que a alocação de memória. Essa sobrecarga da CPU é observada apenas durante o período de interrupção, quando o banco de dados está inacessível e o broker secundário está ativo.

Embora o LocalDB possa usar vários núcleos (até 4), ele é limitado a um único soquete. Adicionar mais soquetes não melhorará o desempenho (por exemplo, ter 4 soquetes com 1 núcleo cada).

Em vez disso, a Citrix recomenda usar vários soquetes com vários núcleos. Nos testes da Citrix, uma configuração 2x3 (2 soquetes, 3 núcleos) proporcionou melhor desempenho do que as configurações 4x1 e 6x1.

### Considerações sobre armazenamento

À medida que os usuários acessam recursos durante uma interrupção, o LocalDB cresce. Por exemplo, durante um teste de logon/logoff executado a 10 logons por segundo, o banco de dados cresceu 1 MB a cada 2-3 minutos. Quando a operação normal é retomada, o banco de dados local é recriado e o espaço é liberado. No entanto, espaço suficiente deve estar disponível na unidade onde o LocalDB está instalado para permitir o crescimento do banco de dados durante uma interrupção. O Cache de Host Local também incorre em mais E/S durante uma interrupção: aproximadamente 3 MB de gravações por segundo, com várias centenas de milhares de leituras.

### Considerações de desempenho

Durante uma interrupção, um broker secundário lida com todas as conexões, então em sites (ou zonas) que fazem balanceamento de carga entre vários Controllers durante operações normais, o broker secundário eleito pode precisar manipular muito mais solicitações do que o normal durante uma interrupção. Portanto, as demandas da CPU serão maiores. Cada broker secundário no site (zona) deve ser capaz de manipular a carga adicional imposta pelo banco de dados do Local Host Cache e todos os VDAs afetados, porque o broker secundário eleito durante uma interrupção pode mudar.

Limites de VDI:

- Em uma implantação VDI de zona única, até 10.000 VDAs podem ser tratados de forma eficaz durante uma interrupção.
- Em uma implantação VDI multizona, até 10.000 VDAs em cada zona podem ser tratados de forma eficaz durante uma interrupção, até um máximo de 40.000 VDAs no site. Por exemplo, cada um dos seguintes sites pode ser tratado de forma eficaz durante uma interrupção:
  - Um site com quatro zonas, cada uma contendo 10.000 VDAs.
  - Um site com sete zonas, uma contendo 10.000 VDAs e seis contendo 5.000 VDAs cada.

Durante uma interrupção, o gerenciamento de carga dentro do site pode ser afetado. Os avaliadores de carga (e especialmente as regras de contagem de sessões) podem ser excedidos.

Durante o tempo que leva para todos os VDAs se registrarem em um broker secundário, esse serviço pode não ter informações completas sobre as sessões atuais. Assim, uma solicitação de conexão de usuário durante esse intervalo pode resultar no lançamento de uma nova sessão,

mesmo que a reconexão a uma sessão existente fosse possível. Este intervalo (enquanto o broker secundário "novo" adquire informações de sessão de todos os VDAs durante o novo registro) é inevitável. As sessões que estão conectadas quando uma interrupção começa não são afetadas durante o intervalo de transição, mas novas sessões e reconexões de sessão podem ser.

Este intervalo ocorre sempre que os VDAs devem se registrar:

- Uma interrupção começa: Ao migrar de um broker principal para um broker secundário.
- Falha do broker secundário durante uma interrupção: Ao migrar de um broker secundário que falhou para um broker secundário recém-eleito.
- Recuperação de uma interrupção: Quando as operações normais são retomadas e o broker principal reassume o controle.

Você pode diminuir o intervalo diminuindo o valor do registro `HeartbeatPeriodMs` do Citrix Broker Protocol (padrão = 600000 ms, o que equivale a 10 minutos). Este valor de heartbeat é o dobro do intervalo que o VDA usa para pings, portanto, o valor padrão resulta em um ping a cada 5 minutos.

Por exemplo, o seguinte comando altera o heartbeat para cinco minutos (300000 milissegundos), o que resulta em um ping a cada 2,5 minutos:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Tenha cuidado ao alterar o valor do heartbeat. Aumentar a frequência resulta em maior carga nos Controladores durante os modos normal e de interrupção.

O intervalo não pode ser totalmente eliminado, independentemente da rapidez com que os VDAs se registrem.

O tempo necessário para sincronizar entre os brokers secundários aumenta com o número de objetos (como VDAs, aplicativos, grupos). Por exemplo, sincronizar 5000 VDAs pode levar 10 minutos ou mais para ser concluído.

### Diferenças das versões do XenApp 6.x

Embora esta implementação do Local Host Cache compartilhe o nome do recurso Local Host Cache no XenApp 6.x e versões anteriores do XenApp, há melhorias significativas. Esta implementação é mais robusta e imune à corrupção. Os requisitos de manutenção são minimizados, como a eliminação da necessidade de comandos periódicos `dsmaint`. Este Local Host Cache é uma implementação tecnicamente diferente.

# Gerenciar o Local Host Cache

Para que o Local Host Cache funcione corretamente, a política de execução do PowerShell em cada Controller deve ser definida como RemoteSigned, Unrestricted ou Bypass.

## SQL Server Express LocalDB

O software Microsoft SQL Server Express LocalDB que o Local Host Cache usa é instalado automaticamente quando você instala um Controller ou atualiza um Controller de uma versão anterior à 7.9. Apenas o broker secundário se comunica com este banco de dados. Você não pode usar cmdlets do PowerShell para alterar nada sobre este banco de dados. O LocalDB não pode ser compartilhado entre Controladores.

O software de banco de dados SQL Server Express LocalDB é instalado independentemente de o Local Host Cache estar ativado.

Para evitar sua instalação, instale ou atualize o Controller usando o comando `XenDesktopServerSetup.exe` e inclua a opção `/exclude "Local Host Cache Storage (LocalDB)"`. No entanto, lembre-se de que o recurso Local Host Cache não funcionará sem o banco de dados, e você não pode usar um banco de dados diferente com o broker secundário.

A instalação deste banco de dados LocalDB não tem efeito sobre a instalação do SQL Server Express para uso como banco de dados do site.

Para obter informações sobre como substituir uma versão anterior do SQL Server Express LocalDB por uma versão mais recente, consulte Substituir SQL Server Express LocalDB.

## Configurações padrão após a instalação e atualização do produto

Durante uma nova instalação do Citrix Virtual Apps and Desktops (versão mínima 7.16), o Local Host Cache é ativado.

Após uma atualização (para a versão 7.16 ou posterior), o Local Host Cache é ativado se houver menos de 10.000 VDAs em toda a implantação.

## Ativar e desativar o Local Host Cache

- Para ativar o Local Host Cache, digite:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Para determinar se o Local Host Cache está ativado, digite `Get-BrokerSite`. Verifique se a propriedade `LocalHostCacheEnabled` é `True`.

- Para desativar o Local Host Cache, digite:

```
Set-BrokerSite -LocalHostCacheEnabled $false
```

Lembre-se: A partir do XenApp e XenDesktop 7.16, o connection leasing (o recurso que precedeu o Local Host Cache a partir da versão 7.6) foi removido do produto e não está mais disponível.

## Verificar se o Local Host Cache está funcionando

Para verificar se o Local Host Cache está configurado e funcionando corretamente:

- Certifique-se de que as importações de sincronização sejam concluídas com sucesso. Verifique os logs de eventos.
- Certifique-se de que o banco de dados SQL Server Express LocalDB foi criado em cada Delivery Controller. Isso confirma que o broker secundário pode assumir, se necessário.
  - No servidor Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
  - Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.
- Force uma interrupção nos Delivery Controllers. Depois de verificar que o Local Host Cache funciona, lembre-se de colocar todos os Controllers de volta no modo normal. Isso pode levar aproximadamente 15 minutos.

## Logs de eventos

Os logs de eventos indicam quando ocorrem sincronizações e interrupções. Nos logs do visualizador de eventos, o modo de interrupção é referido como *modo HA*.*

**Serviço de Sincronização de Configuração:**

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados do Local Host Cache usando o broker do Local Host Cache.

- 503: O Serviço de Sincronização de Configuração do Citrix recebeu uma configuração atualizada. Este evento indica o início do processo de sincronização.
- 504: O Serviço de Sincronização de Configuração do Citrix importou uma configuração atualizada. A importação da configuração foi concluída com êxito.
- 505: O Serviço de Sincronização de Configuração do Citrix falhou em uma importação. A importação da configuração não foi concluída com êxito. Se uma configuração anterior bem-

sucedida estiver disponível, ela será usada em caso de interrupção. No entanto, estará desatualizada em relação à configuração atual. Se não houver configuração disponível anteriormente, o serviço não poderá participar da intermediação de sessão durante uma interrupção. Neste caso, consulte a seção Solução de problemas e entre em contato com o Suporte Citrix.

- 507: O Serviço de Sincronização de Configuração do Citrix abandonou uma importação porque o sistema está em modo de interrupção e o broker do Local Host Cache está sendo usado para intermediação. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque ocorreu uma interrupção. Este é um comportamento esperado.
- 510: Nenhum dado de configuração do Serviço de Configuração recebido do Serviço de Configuração primário.
- 517: Houve um problema na comunicação com o Broker primário.
- 518: O script de Sincronização de Configuração foi abortado porque o Broker secundário (Serviço de Alta Disponibilidade) não está em execução.

**Serviço de Alta Disponibilidade:**

Este serviço também é conhecido como o broker do Local Host Cache.

- 3502: Ocorreu uma interrupção e o broker do Local Host Cache está realizando operações de intermediação.
- 3503: Uma interrupção foi resolvida e as operações normais foram retomadas.
- 3504: Indica qual broker do Local Host Cache é eleito, além de outros brokers do Local Host Cache envolvidos na eleição.
- 3507: Fornece uma atualização de status do Cache de Host Local a cada 2 minutos, que indica que o modo Cache de Host Local está ativo no broker eleito. Contém um resumo da interrupção, incluindo duração da interrupção, registro de VDA e informações da sessão.
- 3508: Anuncia que o Cache de Host Local não está mais ativo no broker eleito e as operações normais foram restauradas. Contém um resumo da interrupção, incluindo duração da interrupção, número de máquinas que se registraram durante o evento do Cache de Host Local e o número de inicializações bem-sucedidas durante o evento LHC.
- 3509: Notifica que o Cache de Host Local está ativo nos brokers não eleitos. Contém uma duração de interrupção a cada 2 minutos e indica o broker eleito.
- 3510: Anuncia que o Local Host Cache não está mais ativo no(s) broker(s) não eleito(s). Contém a duração da interrupção e indica o broker eleito.

## Forçar uma interrupção

Você pode querer forçar deliberadamente uma interrupção.

- Se sua rede estiver caindo e voltando repetidamente. Forçar uma interrupção até que os problemas de rede sejam resolvidos evita a transição contínua entre os modos normal e de interrupção (e as frequentes tempestades de registro de VDA resultantes).
- Para testar um plano de recuperação de desastres.
- Para ajudar a garantir que o Local Host Cache esteja funcionando corretamente.
- Ao substituir ou fazer a manutenção do servidor de banco de dados do site.

Para forçar uma interrupção, edite o registro de cada servidor que contém um Delivery Controller. Em `HKLM\Software\Citrix\DesktopServer\LHC`, crie e defina `OutageModeForced` como `REG_DWORD` para `1`. Essa configuração instrui o broker do Local Host Cache a entrar no modo de interrupção, independentemente do estado do banco de dados. Definir o valor como `0` tira o broker do Local Host Cache do modo de interrupção.

Para verificar eventos, monitore o arquivo de log `Current_HighAvailabilityService` em `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

## Solução de problemas

Várias ferramentas de solução de problemas estão disponíveis quando uma importação de sincronização para o banco de dados do Local Host Cache falha e um evento 505 é publicado.

**Rastreamento CDF:** Contém opções para os módulos `ConfigSyncServer` e `BrokerLHC`. Essas opções, juntamente com outros módulos do broker, provavelmente identificarão o problema.

**Relatório:** Se uma importação de sincronização falhar, você pode gerar um relatório. Este relatório para no objeto que causou o erro. Este recurso de relatório afeta a velocidade de sincronização, então a Citrix recomenda desativá-lo quando não estiver em uso.

Para habilitar e produzir um relatório de rastreamento CSS, digite o seguinte comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

O relatório HTML é publicado em `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`

Após a geração do relatório, digite o seguinte comando para desabilitar o recurso de relatório:

`Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0`

**Exportar a configuração do broker:** Fornece a configuração exata para fins de depuração.

`Export-BrokerConfiguration | Out-File <file-pathname>`

Por exemplo, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

### Comandos PowerShell do Cache de Host Local

Você pode gerenciar o Local Host Cache (LHC) em seus Delivery Controllers usando comandos PowerShell.

O módulo PowerShell está localizado no seguinte caminho nos Delivery Controllers:

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **Importante:**
>
> Execute este módulo apenas nos Delivery Controllers.

#### Importar módulo PowerShell

Para importar o módulo, execute o seguinte no seu Delivery Controller.

`cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1`

#### Comandos PowerShell para gerenciar o LHC

Os comandos a seguir ajudam você a ativar e gerenciar o modo LHC nos Delivery Controllers.

| CMDLETS | FUNÇÃO |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Coloca o Broker no modo LHC. Os arquivos de banco de dados LHC devem ter sido criados com sucesso pelo Serviço ConfigSync para que `Enable-LhcForcedOutageMode` funcione corretamente. Este cmdlet apenas força o LHC no Delivery Controller onde foi executado. Para que o LHC se torne ativo, |

| CMDLETS | FUNÇÃO |
| --- | --- |
| | este comando deve ser executado em todos os Delivery Controllers dentro da zona. |
| `Disable-LhcForcedOutageMode` | Tira o Broker do modo LHC. Este cmdlet apenas desativa o modo LHC no Delivery Controller onde foi executado. `Disable-LhcForcedOutageMode` deve ser executado em todos os Delivery Controllers dentro da zona. |
| `Set-LhcConfigSyncIntervalOverride` | Define o intervalo no qual o Serviço Citrix Config Synchronizer (CSS) verifica as alterações de configuração dentro do site. O intervalo de tempo pode variar de 60 segundos (um minuto) a 3600 segundos (uma hora). Essa configuração se aplica apenas ao Delivery Controller no qual foi executada. Para consistência entre os Delivery Controllers, considere executar este cmdlet em cada Delivery Controller. Por exemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |
| `Clear-LhcConfigSyncIntervalOverride` | Define o intervalo no qual o Serviço Citrix Config Synchronizer (CSS) verifica as alterações de configuração dentro do site para o valor padrão de 300 segundos (cinco minutos). Essa configuração se aplica apenas ao Delivery Controller no qual foi executada. Para consistência entre os Delivery Controllers, considere executar este cmdlet em cada Delivery Controller. |
| `Enable-LhcHighAvailabilitySDK` | Habilita o acesso a todos os cmdlets `Get-Broker*` dentro do Delivery Controller no qual foi executado. |
| `Disable-LhcHighAvailabilitySDK` | Desabilita o acesso aos cmdlets do Broker dentro do Delivery Controller no qual foi executado. |

**Nota:**

- Use a porta 89 ao executar os cmdlets `Get-Broker*` no Delivery Controller. Por exemplo:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- Quando não está no modo LHC, o Broker LHC no Delivery Controller contém apenas informações de configuração.
- Durante o modo LHC, o Broker LHC no Delivery Controller eleito contém as seguintes informações:
  - Estados dos recursos
  - Detalhes da sessão
  - Registros de VDA
  - Informações de configuração

# Monitorar e gerenciar máquinas e sessões usando Pesquisa

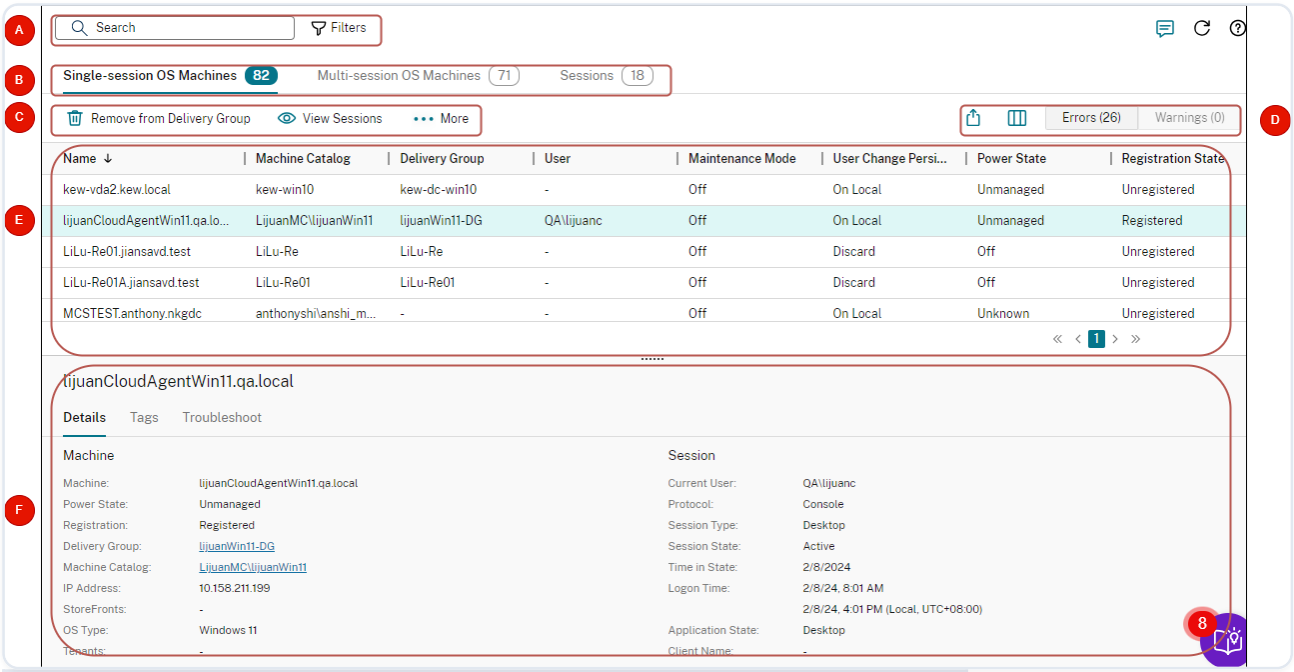
**Observação:**

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

Este artigo o orienta sobre como monitorar e gerenciar máquinas e sessões usando o nó **Pesquisa** no Web Studio.

## Saiba mais sobre o nó

O nó **Pesquisa** fornece um local central para monitorar e gerenciar máquinas e sessões de usuário.




| CHAMADA | ÁREA | DESCRIÇÃO |
|---|---|---|
| A | Barra de pesquisa | Fornece uma pesquisa rápida e uma pesquisa baseada em filtro que permite definir critérios de pesquisa complexos. Para obter mais informações, consulte Pesquisar instâncias. |
| B | Guias de tipo | Exibe guias para listar máquinas por tipo ou listar todas as sessões. As contagens de instâncias aparecem nos nomes das guias. |
| C | Ações no nível da instância | Exibe as ações que você pode realizar nas *instâncias selecionadas* (máquinas ou |

| CHAMADA | ÁREA | DESCRIÇÃO |
| --- | --- | --- |
| | | sessões). Para obter mais informações, consulte Ações da máquina e Ações da sessão. |
| D | Ações no nível da lista | Exibe as ações que você pode executar na *lista* atual<br>• Ícone de **Exportar**: Exporta a lista de instâncias exibidas na visualização principal para um arquivo CSV.<br>• Ícone **Coluna a ser exibida**: Personalize a exibição principal da lista.<br>• Rótulo **Erros**: Ative este rótulo para exibir apenas máquinas não registradas com erros na exibição principal. Para visualizar os detalhes do |

| CHAMADA | ÁREA | DESCRIÇÃO |
| --- | --- | --- |
| | | problema, vá para a guia **Solucionar problemas** no painel **Detalhes**.<br>• Rótulo **Aviso**: Ative este rótulo para exibir apenas máquinas não registradas com avisos na exibição principal. Para visualizar os detalhes do problema, vá para a guia **Solucionar problemas** no painel **Detalhes**. |
| E | Exibição principal | Exibe as instâncias e suas propriedades. Você pode personalizar a exibição principal selecionando o ícone **Coluna a ser exibida**. Para obter mais informações sobre as colunas disponíveis, consulte Colunas da máquina e Colunas da sessão. |

| CHAMADA | ÁREA | DESCRIÇÃO |
| --- | --- | --- |
| F | Painel de detalhes | Exibe os seguintes detalhes:<br>• Detalhes da instância selecionada (máquina ou sessão)<br>• Tags aplicadas à máquina selecionada<br>• Detalhes de erros ou avisos com a máquina selecionada, incluindo problemas, possíveis causas e soluções sugeridas |

## Pesquisar instâncias

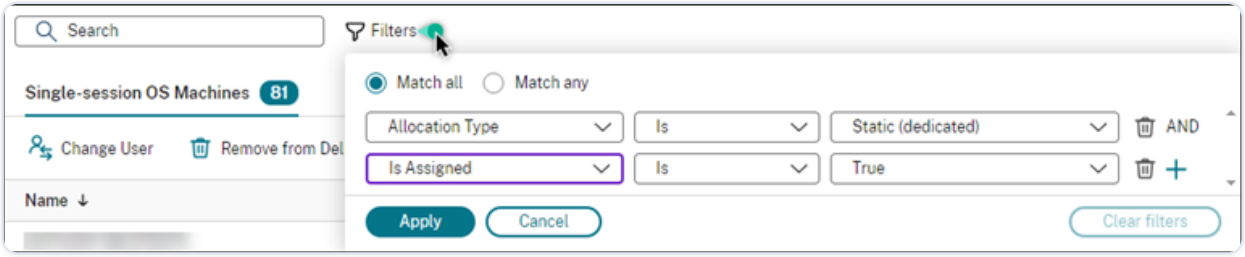
Use a função de pesquisa para localizar máquinas e sessões específicas:

- Pesquisar usando filtros
- Salvar o conjunto de filtros atual para uma pesquisa rápida
- Fixar um campo de filtro na barra de pesquisa
- Pesquisar usando a caixa de pesquisa rápida
- Dicas para aprimorar uma pesquisa

### Pesquisar usando filtros

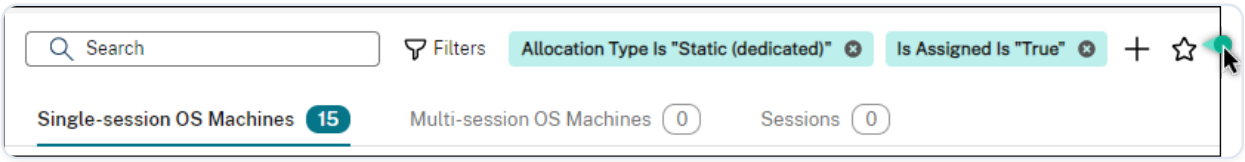
Por exemplo, para localizar todas as máquinas OS de sessão única que são *estáticas* e *atribuídas a usuários*, siga estas etapas:

1. Na guia **Máquinas OS de sessão única**, clique no ícone **Filtros**. O painel Filtros é exibido.
2. Adicione os critérios de filtro necessários.




3. Selecione **Corresponder a todos** (operador AND) se quiser que a pesquisa retorne resultados que correspondam a todos os critérios de filtro. Selecione **Corresponder a qualquer um** (operador OR) se quiser que a pesquisa retorne resultados que correspondam a qualquer um dos critérios de filtro.
4. Clique em **Aplicar**.

   A lista filtrada exibe todas as máquinas OS de sessão única que são estáticas e atribuídas a usuários.

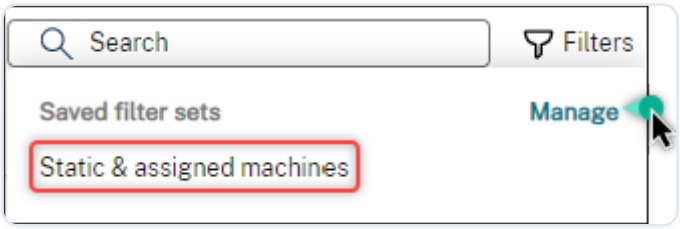



### Salvar o conjunto de filtros atual para uma pesquisa rápida

Por exemplo, para salvar o conjunto de filtros para máquinas OS de sessão única que são estáticas e atribuídas a usuários para uso futuro, siga estas etapas:

1. Depois de realizar uma pesquisa baseada em filtro, clique no ícone **Estrela** na barra de pesquisa, conforme mostrado na figura anterior.
2. Na página que aparece, insira um nome para este conjunto de filtros (por exemplo, *Máquinas estáticas e atribuídas*).
3. Clique em **Salvar**.

   O conjunto de filtros salvo aparece na lista de histórico de pesquisa quando você clica na caixa de pesquisa.



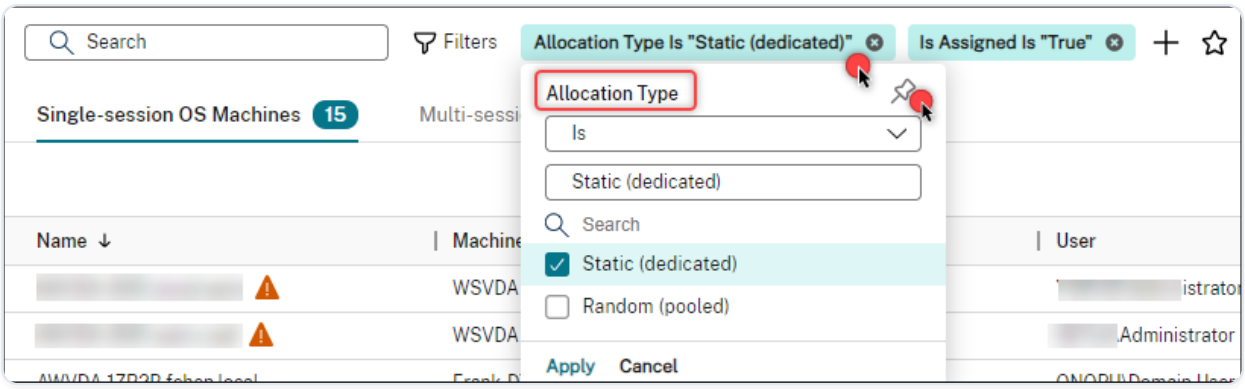

**Observação:**

Conjuntos de filtros são salvos por conta de usuário. Para gerenciar conjuntos de filtros salvos, selecione **Gerenciar**.

### Fixar um campo de filtro na barra de pesquisa

Fixe *campos* de filtro usados com frequência na barra de pesquisa para facilitar o acesso. Por exemplo, após realizar uma pesquisa baseada em filtro, você deseja fixar **Tipo de Alocação** na barra de pesquisa. Siga estas etapas:

1. Clique na *configuração de filtro* na barra de pesquisa.
2. No painel que aparece, clique no ícone **Fixar** para fixar o campo de filtro (*Tipo de Alocação* para este exemplo) na barra de pesquisa.




### Pesquisar usando a caixa de pesquisa rápida

A caixa de pesquisa rápida oferece uma maneira conveniente de pesquisar instâncias com base em propriedades relacionadas ao nome ou conjuntos de filtros salvos. As etapas detalhadas são as seguintes:

1. Clique na caixa de pesquisa. Suas pesquisas recentes e conjuntos de filtros salvos aparecem na lista suspensa. Você pode clicar em uma pesquisa anterior ou conjunto de filtros para uma pesquisa rápida.
2. Para iniciar uma nova pesquisa, insira um nome completo ou parcial das seguintes opções:

- Nome da máquina ou nome DNS
- Nome do catálogo de máquinas
- Nome do grupo de entrega
- Nome de usuário da sessão
- Nome do cliente da sessão
- Nome amigável da VM que hospeda a sessão, conforme usado pelo seu hipervisor
- Nome do servidor de hospedagem

### Dicas para aprimorar uma pesquisa

Considere as seguintes dicas ao usar o recurso Pesquisar:

- No nó **Pesquisar**, selecione qualquer coluna para classificar os itens.
- Para mostrar mais características a serem incluídas na exibição onde você pode pesquisar e classificar, selecione **Colunas a Exibir** ou clique em qualquer coluna e selecione **Colunas a Exibir**. Na janela **Colunas a Exibir**, marque a caixa de seleção ao lado dos itens que deseja exibir e selecione **Salvar** para sair.

> **Observação:**
>
> As colunas que degradam o desempenho são marcadas com o rótulo **Degrada o desempenho**.

- Para localizar um dispositivo de usuário conectado a uma máquina, use **Cliente (IP)** e **É**, e insira o endereço IP do dispositivo.
- Para localizar sessões ativas, use **Estado da Sessão**, **É** e **Conectado**.
- Para listar todas as máquinas em um grupo de entrega, selecione **Grupos de Entrega** no painel esquerdo. Selecione o grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações ou no menu de contexto.

Tenha as seguintes considerações em mente ao realizar operações de classificação:

- Enquanto o número de itens não exceder 5.000, você pode clicar em qualquer coluna para classificar os itens nela. Quando o número exceder 5.000, você só poderá classificar por nome ou por usuário atual (dependendo da guia em que você está). Para habilitar a classificação, use filtros para reduzir o número de itens para 5.000 ou menos.

- Quando o número de itens for maior que 500, mas não mais que 5.000:
  - Armazenamos todos os dados em cache localmente para melhorar o desempenho da classificação. Nas guias **Máquinas OS de sessão única** e **Máquinas OS de várias sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Nome**) para classificar. Na guia **Sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Usuário Atual**) para classificar. Como resultado, a classificação leva mais tempo para ser concluída. Para um desempenho mais rápido, classifique por nome ou usuário atual, ou use filtros para reduzir o número de itens.
  - A seguinte mensagem abaixo da tabela indica que os dados estão em cache: Última atualização: `<the time when you refreshed the table>`. Nesse caso, as operações de classificação são baseadas em itens que foram carregados anteriormente. Esses itens podem não estar atualizados. Para atualizá-los, clique no ícone de atualização.

## Personalizar colunas a serem exibidas

Crie uma exibição principal personalizada para exibir as propriedades e status cruciais para suas operações diárias. As etapas detalhadas são as seguintes:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS de várias sessões**, **Máquinas OS de sessão única** ou **Sessões**, conforme necessário.
2. Clique no ícone **Colunas a serem exibidas** na barra de ações e selecione as colunas.

   Para obter mais informações sobre as colunas disponíveis e suas descrições, consulte Colunas da máquina e Colunas da sessão.

Ao escolher as colunas, você pode ver colunas marcadas com o rótulo **Degrada o desempenho**. A seleção dessas colunas pode degradar o desempenho do console. Tenha estas considerações em mente:

- Depois de concluir sua personalização, a tabela é atualizada para exibir as colunas selecionadas. A presença delas pode resultar em atrasos ao atualizar a tabela.
- Depois de atualizar o navegador ou sair do console e fazer login novamente, uma mensagem aparece perguntando se deseja preservar essas colunas. Se você optar por preservá-las, estará restrito a atualizar a tabela mais de uma vez por minuto para um desempenho ideal do console. Para atualizações mais frequentes, remova todas as colunas que degradam o desempenho.

# Gerenciar máquinas e sessões

Use as ações no nó Pesquisar para solucionar problemas de máquinas e sessões ou processar solicitações de usuários.

## É bom saber

Você pode gerenciar máquinas em diferentes níveis:

- No nível da máquina individual. Use o nó **Pesquisar** para localizar máquinas de destino e executar ações.
- No nível do catálogo de máquinas, como alterar imagens mestre para um catálogo, excluir máquinas de um catálogo e adicionar máquinas a um catálogo. Para obter mais informações, consulte Gerenciar catálogos de máquinas.
- No nível do grupo de entrega, como ativar ou desativar o modo de manutenção para máquinas em um grupo. Para obter mais informações, consulte Gerenciar grupos de entrega.

Além do nível de sessão individual, você também pode gerenciar sessões no nível do grupo de entrega, como configurar o pré-lançamento e a permanência da sessão para um grupo de entrega. Para obter mais informações, consulte Gerenciar Grupos de Entrega.

## Executar ações em máquinas ou sessões

Para gerenciar máquinas ou sessões no nível da instância individual, siga estas etapas:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS multissessão**, **Máquinas OS de sessão única** ou **Sessões**.
2. Selecione uma ou mais instâncias conforme necessário.
3. Na barra de ações ou no menu de clique com o botão direito, selecione uma ação com base nos problemas que você encontrar com essas instâncias ou nas solicitações do usuário.

   Para obter mais informações sobre as ações disponíveis e suas descrições, consulte Ações da máquina e Ações da sessão.

> **Observação:**
>
> Se você selecionar duas ou mais instâncias, somente as ações que se aplicam a todas elas estarão disponíveis.

## Exportar dados de máquina ou sessão para arquivos CSV

Exporte a lista de instâncias (máquinas ou sessões) exibidas em uma guia (até 30.000 itens) para um arquivo CSV. As etapas detalhadas são as seguintes:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS de várias sessões**, **Máquinas OS de sessão única** ou **Sessões**, conforme necessário.
2. Clique no ícone **Exportar** no canto superior direito.
3. Na caixa de diálogo que aparece, clique em **Continuar**.

   A exportação pode levar vários minutos para ser concluída. Você pode encontrar o arquivo na pasta de download padrão do seu navegador.

> **Observação:**
>
> Em cada guia do nó **Pesquisar**, você não pode realizar outra exportação enquanto uma exportação estiver em andamento.

## Ações e colunas da máquina

Este artigo lista ações e colunas de máquina com descrições para sua referência.

### Ações

Visualize as ações que você pode realizar em máquinas e suas descrições.

| AÇÃO | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Remover do Grupo de Entrega | Remove uma máquina do grupo de entrega. | Sessão única e multissessão |
| Adicionar ao Grupo de Entrega | Adiciona uma máquina a um grupo de entrega. | Sessão única e multissessão |
| Exibir Sessões | Exibir as sessões em execução em uma máquina | Sessão única e multissessão |
| Gerenciar Tags | Adicione e gerencie tags para uma máquina. Para obter mais informações sobre | Sessão única e multissessão |

| AÇÃO | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| | casos de uso típicos de tags, consulte Tags. | |
| Ativar Modo de Manutenção | Coloque uma máquina em modo de manutenção antes de aplicar patches ou para solução de problemas. | Sessão única e multissessão |
| | Este modo impede que novas conexões sejam feitas a essa máquina. Os usuários podem se conectar a sessões existentes nessa máquina, mas não podem iniciar novas sessões nela. | |
| Desativar Modo de Manutenção | Desative o modo de manutenção para uma máquina. | Sessão única e multissessão |
| Atualizar VDA | Atualizar VDA para uma máquina. | Máquinas de SO de sessão única ou multissessão que atendem a determinados requisitos: Saiba mais. |
| Fazer logoff | Forçar logoff de uma máquina | Sessão única e multissessão |
| Excluir | Excluir uma VM de um catálogo de máquinas, deixando-a intacta no hipervisor ou serviço de nuvem. | Sessão única e multissessão |
| Alterar Usuário | Atribuir uma máquina a um usuário específico. | máquinas *estáticas* de sessão única. |
| Iniciar | Iniciar uma máquina. | Sessão única e multissessão |
| Desligar | Desligar uma máquina. | Sessão única e multissessão |
| Reiniciar | Reiniciar uma máquina | Sessão única e multissessão |

| AÇÃO | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Suspender | Coloque uma máquina em estado de hibernação ou suspensão. Ao suspender uma máquina, os Delivery Controllers armazenam o conteúdo da memória da máquina em um arquivo e, em seguida, desligam a máquina. | Máquinas OS de sessão única |
| Retomar | Retome uma máquina suspensa. Ao retomar uma máquina suspensa, os Delivery Controllers iniciam a máquina e a restauram para o estado anterior. | Máquinas OS de sessão única |
| Forçar Reinicialização | Forçar a reinicialização de uma máquina. | Máquinas OS de sessão única |
| Forçar Desligamento | Forçar o desligamento de uma máquina. | Máquinas OS de sessão única |

## Colunas

Visualize todas as colunas da máquina e suas descrições por tipo:

- Máquina
- Detalhes da máquina
- Aplicativos
- Hospedagem
- Conexão
- Registro
- Detalhes da Sessão
- Sessão

### Máquina

Colunas na categoria **Máquina**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| Nome | O nome de host DNS da máquina. | Sessão única e multissessão |
| Catálogo de Máquinas | O nome do catálogo ao qual a máquina pertence. | Sessão única e multissessão |
| Grupo de Entrega | O nome do grupo de entrega ao qual a máquina pertence. | Sessão única e multissessão |
| Nome de Exibição do Usuário | Os nomes completos dos usuários associados à máquina (geralmente no formato `Firstname Lastname`). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas. | Sessão única e multissessão |
| Usuário | Os nomes de usuário dos usuários associados à máquina (no formato “domínio\usuário”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas. | Sessão única e multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| Nome Principal do Usuário | Os Nomes Principais de Usuário dos usuários associados à máquina (no formato “usuário@domínio”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas. | Sessão única e multissessão |
| Nome de Exibição da Área de Trabalho | O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix Workspace™ ou no StoreFront.<br><br>**Nota:** Para alterar a exibição de um desktop, você precisa da permissão **Perform Machine Update** porque a alteração do nome de exibição envolve a atualização da propriedade da máquina. | Somente sessão única |
| Condições do Desktop | A lista de condições pendentes do desktop para a máquina. Valores | Sessão única e multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | possíveis: Unknown, CPU, ICALatency e UPMLogonTime. | |
| Tipo de Alocação | O tipo de alocação da máquina: **Permanente**, quando alocada a um usuário permanentemente. **Aleatória**, quando alocada aleatoriamente. | Sessão única e multissessão |
| Modo de Manutenção | Indica se a máquina está no modo de manutenção. | Sessão única e multissessão |
| Configuração de Conexão do Windows | Modo de logon relatado pelo Windows. | Somente multissessão |
| | Valores possíveis: LogonEnabled, Draining, DrainingUntilRestart e LogonDisabled. | |
| Está Atribuído | Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/ endereço). Os usuários podem ser atribuídos explicitamente ou por atribuição no primeiro uso da máquina. | Sessão única e multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| É Físico | Indica se a máquina é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada por energia pelos Delivery Controllers. `False` indica o contrário. | Sessão única e multissessão |
| Tipo de Provisionamento | Como a máquina foi provisionada. Valores possíveis:<br>• Manual: Não provisionado usando PVS ou MCS. | Sessão única e multissessão |
| | PVS: Provisionado usando PVS (máquinas físicas, blade e virtuais) | |
| | MCS: Provisionado usando MCS (somente VMs) | |
| Reinicialização Agendada | O estado de qualquer operação de reinicialização agendada para a máquina. Valores possíveis | Sessão única e multissessão |
| | Nenhum: Nenhuma reinicialização está agendada. | |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | Pendente: Aguardando reinicialização, mas está disponível para uso.<br>• Drenando: Aguardando reinicialização e está indisponível para novas sessões. No entanto, reconexões a conexões existentes ainda são permitidas.<br>• Em Andamento: Em andamento ativo de uma reinicialização agendada.<br>• Natural: Reinicialização natural em andamento. A máquina está aguardando uma reinicialização. | |
| Zona | O nome da zona onde a máquina está localizada. | Sessão única e multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Estado | O estado geral da área de trabalho associada à máquina, derivado de vários estados específicos, como estado da sessão, estado de registro e estado de energia. | Sessão única e multissessão |
| | Estados possíveis: Desligado, Não Registrado, Disponível, Desconectado, EmUso e Preparando. | |
| Tags | A lista de tags associadas à máquina. | Sessão única e multissessão |
| Atualização do VDA | O estado da máquina para ações de atualização de pacote VDA. | Sessão única e multissessão |
| | Valores possíveis: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate e Unknown. | |
| Capaz de Suspender | Indica se a máquina suporta ações de energia (Suspender e Retomar). | Sessão única e multissessão |
| Índice de Carga | O índice de carga atual. Para obter | Somente multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| | mais informações, consulte Saiba mais. | |
| Estado de Esvaziamento | Indica se a máquina está esvaziando e será desligada após o término de todas as sessões na máquina. 'True' aparece apenas para máquinas multissessão gerenciadas por energia. | Somente multissessão |
| | **Nota:** A máquina não desliga se estiver em modo de manutenção. Ela desliga somente depois de sair do modo de manutenção. | |

### Detalhes da máquina

Colunas na categoria **Detalhes da máquina**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Versão do Agente | A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina. | Sessão única e multi-sessão |
| Endereço IP | O endereço IP da máquina. | Sessão única e multi-sessão |
| Atribuído | Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/endereço). Os usuários podem ser atribuídos explicitamente ou | Sessão única e multi-sessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | por atribuição no primeiro uso da máquina. | |
| Tipo de SO | O tipo de sistema operacional em execução na máquina. | Somente sessão única |

### Aplicativos

Colunas na categoria **Aplicativos**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| Aplicativo em Uso | A lista de aplicativos em uso na máquina (exibidos como nomes de navegador). | Sessão única e multissessão |
| Aplicativos Publicados | A lista de aplicativos publicados pela máquina (exibidos como nomes de navegador). | Sessão única e multissessão |

### Conexões

Colunas na categoria **Conexões**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| Cliente (IP) | O endereço IP do cliente conectado à máquina. | Somente sessão única |
| Cliente | O nome do host do cliente conectado à máquina. | Somente sessão única |
| Versão do Plug-In | A versão do aplicativo Citrix Workspace no cliente conectado. | Somente sessão única |
| Conectado Via | O nome do host da conexão de entrada, geralmente um gateway, roteador ou cliente. | Somente sessão única |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Conectado Via (IP) | O endereço IP da conexão de entrada, geralmente um gateway, roteador ou cliente. | Somente sessão única |
| Tipo de Conexão | O protocolo usado para a sessão. Valores possíveis: HDX, RDP e Console. Nota: O campo é deixado em branco para sessões de console em VDAs do XenDesktop® 5. | Somente sessão única |
| Hora da Última Conexão (UTC) | A hora da última tentativa de conexão detectada que falhou ou foi bem-sucedida. | Sessão única e multissessão |
| Último Usuário de Conexão | O nome SAM (no formato “DOMÍNIO\usuário”) do usuário que tentou uma conexão com a máquina pela última vez. Se o nome SAM não estiver disponível, o SID será usado. | Sessão única e multissessão |
| Secure ICA® Ativo | Indica se o SecureICA está ativo na sessão atual. Sempre nulo para máquinas multissessão. | Sessão única e multissessão |

### Hospedagem

Colunas na categoria **Hospedagem**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| VM | O nome amigável de uma máquina hospedada executando a sessão, conforme usado por seu | Sessão única e multi-sessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | hipervisor. Não corresponde necessariamente ao nome DNS ou AD da máquina. | |
| Nome do Servidor de Hospedagem | O nome DNS do hipervisor que está hospedando a máquina, se gerenciado. | Sessão única e multi-sessão |
| Conexão | O nome da conexão do host atribuída à máquina que hospeda a sessão. | Sessão única e multi-sessão |
| Atualização Pendente | Indica se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina. | Sessão única e multi-sessão |
| Persistência de Alterações do Usuário | Como as alterações do usuário são tratadas, indicando se as alterações são persistentes:<br>• OnLocal: Persistente. As alterações do usuário são salvas localmente. | Sessão única e multi-sessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | • Descartar: Não persistente. As alterações do usuário são descartadas. | |
| Ação de Energia Pendente | Indica se há alguma ação de energia pendente para a máquina. | Sessão única e multi-sessão |
| Estado de Energia | O estado de energia da máquina. Valores possíveis: Não gerenciado, Desconhecido, Indisponível, Desligado, Ligado, Suspenso, Ligando, Desligando, Suspendendo e Retomando. | Sessão única e multi-sessão |
| Será Desligado Após o Uso | Aplicável apenas a máquinas de sessão única gerenciadas por energia. Indica se a máquina está comprometida e será desligada após o término de todas as sessões.<br><br>**Observação:** A máquina não será desligada se estiver em modo de manutenção. Ela será desligada somente depois que | Somente sessão única |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | for retirada do modo de manutenção. | |

### Registro

Colunas na categoria **Registro**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| Última Falha de Registro | O motivo da última desativação do registro da máquina com o broker. | Sessão única e multissessão |
| | Os valores possíveis são: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, | |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
| --- | --- | --- |
| | FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError e BrokerRegistrationLimitReached. | |
| Hora da Última Falha de Registro (UTC) | A hora da última desativação do registro da máquina. | Sessão única e multissessão |
| Estado do Registro | O estado de registro da máquina. Valores possíveis: Não registrado, Inicializando, Registrado e Erro do Agente. | Sessão única e multissessão |
| Estado de Falha | O estado de resumo de qualquer estado de falha atual da máquina. Valores possíveis:<br>• Nenhum: Nenhuma falha. | Sessão única e multissessão |

| COLUNA | DESCRIÇÃO | APLICA-SE A | |
|---|---|---|---|
| | A máquina está íntegra.<br>• FalhaAoIniciar: A última operação de inicialização da máquina falhou.<br>• TravadoNaInicialização: A máquina não conseguiu iniciar após ser ligada.<br>• Não registrado. A máquina falhou ao registrar dentro do período esperado ou seu registro foi rejeitado.<br>• Capacidade Máxima. A máquina está se reportando com capacidade máxima. | | |

### Detalhes da sessão

Colunas na categoria **Detalhes da sessão**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Iniciado por | O nome do host do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão. | Sessão única e multissessão |
| Iniciado por (IP) | O endereço IP do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão. | Sessão única e multissessão |
| Hora da Alteração da Sessão (UTC) | A hora da última alteração de estado da sessão atual. | Somente sessão única |
| Filtros SmartAccess | Tags Smart Access para a sessão atual. Sempre nulo para máquinas multissessão. | Sessão única e multissessão |

### Sessão

Colunas na categoria **Sessão**.

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Estado da Sessão | O estado da sessão atual. Valores possíveis: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession e Unknown. | Somente sessão única |
| Usuário Atual | O nome do usuário da sessão atual (no formato “DOMAIN\user”). | Somente sessão única |
| Hora de Início (UTC) | A hora de início da sessão atual. | Somente sessão única |

| COLUNA | DESCRIÇÃO | APLICA-SE A |
|---|---|---|
| Contagem de Sessões | O número de sessões na máquina. | Somente multissessão |

## Ações e colunas da sessão

Este artigo lista as ações e colunas da máquina com descrições para sua referência.

### Ações

Visualize as ações que você pode realizar nas sessões e suas descrições.

| AÇÃO | DESCRIÇÃO | APLICA-SE A SESSÕES EM |
|---|---|---|
| Fazer logoff | Desconectar um usuário de uma sessão. | Máquinas OS de sessão única ou máquinas OS de múltiplas sessões |
| Enviar Mensagem | Enviar uma mensagem para o usuário de uma sessão. | Máquinas OS de sessão única ou máquinas OS de múltiplas sessões |
| Visualizar máquinas | Visualizar a máquina host de uma sessão. | Máquinas OS de sessão única ou máquinas OS de múltiplas sessões |
| Desconectar | Desconectar uma sessão. Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com os Delivery Controllers. | Máquinas OS de sessão única ou máquinas OS de múltiplas sessões |
| Desligar Máquina | Desliga a máquina associada a uma sessão. | Máquinas OS de sessão única |
| Reiniciar Máquina | Reinicia a máquina associada a uma sessão. | Máquinas OS de sessão única |

## Colunas

Exibir colunas da sessão e suas descrições.

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Usuário atual | O nome do usuário; o Nome Principal do Usuário (UPN) do usuário. |
| Nome | O nome do host DNS da máquina que hospeda a sessão. |
| Grupo de Entrega | O nome do grupo de entrega que contém a máquina que hospeda a sessão. |
| Catálogo de Máquinas | O nome do catálogo de máquinas que contém a máquina que hospeda a sessão. |
| Versão do Agente | A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina que hospeda a sessão. |
| Aplicativo em Uso | A lista de aplicativos em uso na sessão, identificados por seus nomes administrativos. |
| Intermediação Autônoma | Indica se esta é uma sessão HDX™ estabelecida por uma conexão direta sem intermediação. |
| Hora da Intermediação (UTC) | A hora em que a sessão foi intermediada. |
| Nome de Usuário do Intermediador | O nome do usuário intermediador. |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Cliente (IP) | O endereço IP do cliente conectado à sessão. |
| Cliente | O nome do host do cliente conectado à sessão. |
| Versão do Plug-In | A versão do aplicativo Citrix Workspace™ em execução no cliente conectado à sessão. |
| Conectado Via | O nome do host das conexões de entrada, tipicamente um gateway, roteador ou cliente. |
| Conectado Via (IP) | O endereço IP da conexão de entrada, geralmente um gateway, roteador ou cliente. |
| Tipo de Alocação | Se a sessão é compartilhada ou dedicada. |
| Oculto | Se a sessão está oculta para o usuário e não deve ser reconectada. |
| VM | O nome amigável da VM que hospeda a sessão, conforme usado por seu hipervisor. Não corresponde necessariamente ao nome DNS ou AD da máquina. |
| Nome do Servidor de Hospedagem | O nome DNS do hipervisor que está hospedando a máquina de hospedagem da sessão. |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Conexão | O nome da conexão do host atribuída à máquina que hospeda a sessão. |
| Atualização Pendente | Se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina. |
| Modo de Manutenção | Se a máquina que hospeda a sessão está em modo de manutenção. |
| Endereço IP | O endereço IP da máquina que hospeda a sessão. |
| É Físico | Se a máquina que hospeda a sessão é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada em termos de energia pelos Delivery Controllers. `False` indica o contrário. |
| Iniciado por | O nome do host do servidor StoreFront™ usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace. |
| Iniciado por (IP) | O endereço IP do servidor StoreFront usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace. |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Tipo de SO | A string de identificação do sistema operacional que hospeda a sessão. |
| Persistência de Alterações do Usuário | Como as alterações do usuário são tratadas, indicando se as alterações são persistentes:<br>• OnLocal: Persistente. As alterações do usuário são salvas localmente.<br>• Descartar: Não persistente. As alterações do usuário são descartadas. |
| Tipo de Conexão | O protocolo usado para a sessão, como HDX, RDP ou Console.<br>**Nota:** O campo fica em branco para sessões de console em VDAs do XenDesktop® 5. |
| Tipo de Provisionamento | Como a máquina que hospeda a sessão foi provisionada:<br>• Manual: Não provisionado usando PVS ou MCS.<br>• PVS: Provisionado por PVS (máquinas físicas, blade e virtuais). |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| | • MCS: Provisionado por MCS (somente VMs). |
| Secure ICA® Ativo | Se o SecureICA está ativo na sessão. |
| Estado da Sessão | O estado da sessão. Valores possíveis: Connected, Active ou Disconnected. Outros estados podem ocorrer para sessões em máquinas com níveis funcionais anteriores a L7, como PreparingSession, Reconnecting, NonBrokeredSession, Other e Unknown. |
| Hora da Alteração da Sessão | A hora da alteração de estado mais recente para a sessão. |
| Estado do Aplicativo | O estado dos aplicativos na sessão. Valores possíveis: PreLogon, PreLaunched, Active, Desktop, Lingering e NoApps. |
| Suporte a Sessão | Se a máquina que hospeda a sessão suporta sessões múltiplas ou únicas. |
| Zona | Nome da zona onde a máquina que hospeda a sessão está localizada. |
| Filtros SmartAccess | Tags de Smart Access para a sessão. |
| Hora de Início (UTC) | Quando a sessão foi iniciada. |

| COLUNA | DESCRIÇÃO |
| --- | --- |
| Estado | O estado de resumo da máquina. Valores possíveis: Não Registrado, Desconectado ou Em Uso. |
| Tempo no Estado (UTC) | Há quanto tempo a sessão está em seu estado atual. |
| Delivery Controller™ | O nome de host DNS do controlador ao qual a máquina que hospeda a sessão está registrada. |
| Nome de Exibição do Usuário | O nome completo do usuário. |
| Nome de Exibição da Área de Trabalho | O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix Workspace ou StoreFront. Para sessões de aplicativo, é o nome do primeiro aplicativo iniciado na sessão, mesmo que esse aplicativo já tenha sido encerrado. O nome permanece inalterado mesmo que o recurso seja posteriormente renomeado ou removido. |

# Gerenciar chaves de segurança

**Importante:**

- Você deve usar este recurso em combinação com o StoreFront™ 1912 LTSR CU2 ou posterior.

- O recurso Secure XML é compatível apenas com o Citrix ADC e o Citrix Gateway versão 12.1 e posterior.

**Nota:**

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

Este recurso permite que você permita que apenas máquinas StoreFront e Citrix Gateway aprovadas se comuniquem com os Delivery Controllers. Depois de habilitar este recurso, todas as solicitações que não contiverem a chave serão bloqueadas. Use este recurso para adicionar uma camada extra de segurança para proteger contra ataques originados da rede interna.

Um fluxo de trabalho geral para usar este recurso é o seguinte:

1. Habilite o Web Studio para mostrar as configurações do recurso.
2. Configure as configurações para o seu site.
3. Configure as configurações para o StoreFront.
4. Configure as configurações para o Citrix ADC.

## Configurar configurações para o site

Você pode usar o Web Studio ou o PowerShell para configurar as configurações da chave de segurança para o seu site.

### Usar o Web Studio

1. Faça login no Web Studio, selecione **Settings** no painel esquerdo.
2. Localize o bloco **Manage security key** e clique em **Edit**. A página **Manage Security Key** é exibida.

   Assistente de Gerenciamento de Chave de Segurança(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/manage-security-key-wizard.png)
3. Clique no ícone de atualização para gerar as chaves.

**Importante:**

- Existem duas chaves disponíveis para uso. Você pode usar a mesma chave ou chaves diferentes para comunicações pelas portas XML e STA. Recomendamos que você use apenas uma chave por vez. A chave não utilizada é usada apenas para rotação de chaves.
- Não clique no ícone de atualização para atualizar a chave já em uso. Se o fizer, ocorrerá interrupção do serviço.

4. Selecione onde uma chave é necessária para comunicações:
   - **Exigir chave para comunicações pela porta XML (somente StoreFront)**. Se selecionado, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta XML, consulte o artigo da Central de Conhecimento CTX127945.
   - **Exigir chave para comunicações pela porta STA**. Se selecionado, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta STA, consulte o artigo da Central de Conhecimento CTX101988.
5. Clique em **Salvar** para aplicar suas alterações e fechar a janela.

### Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações do Web Studio.

1. Execute o SDK remoto do PowerShell do Citrix Virtual Apps and Desktops.
2. Em uma janela de comando, execute o seguinte comando:
   - `Add-PSSnapIn Citrix*`
3. Execute os seguintes comandos para gerar uma chave e configurar a Chave1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Execute os seguintes comandos para gerar uma chave e configurar a Chave2:
   - `New-BrokerXmlServiceKey`

- `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. Execute um ou ambos os comandos a seguir para habilitar o uso de uma chave na autenticação de comunicações:
   - Para autenticar comunicações pela porta XML:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Para autenticar comunicações pela porta STA:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

## Configurar as definições para o StoreFront

Após concluir a configuração do seu site, você precisa configurar as configurações relevantes para o StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos PowerShell:

Para configurar a chave para comunicações pela porta XML, use o comando . Por exemplo:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Insira os valores apropriados para os seguintes parâmetros:

- `Path to store`
- `Resource feed name`
- `secret`

Para configurar a chave para comunicações sobre a porta STA, use os comandos `New-STFSecureTicketAuthority` e `Set-STFRoamingGateway`. Por exemplo:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Insira os valores apropriados para os seguintes parâmetros:

- `Gateway name`
- `STA URL`
- `Secret`

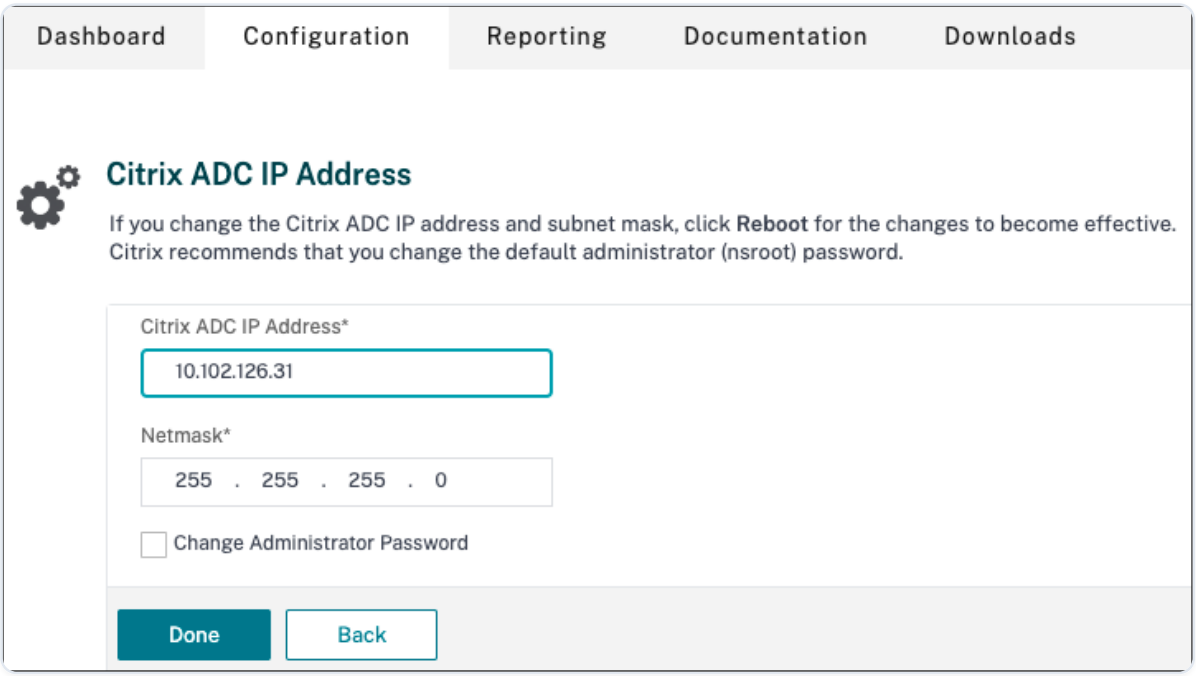
Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

## Configurar as definições para o Citrix ADC

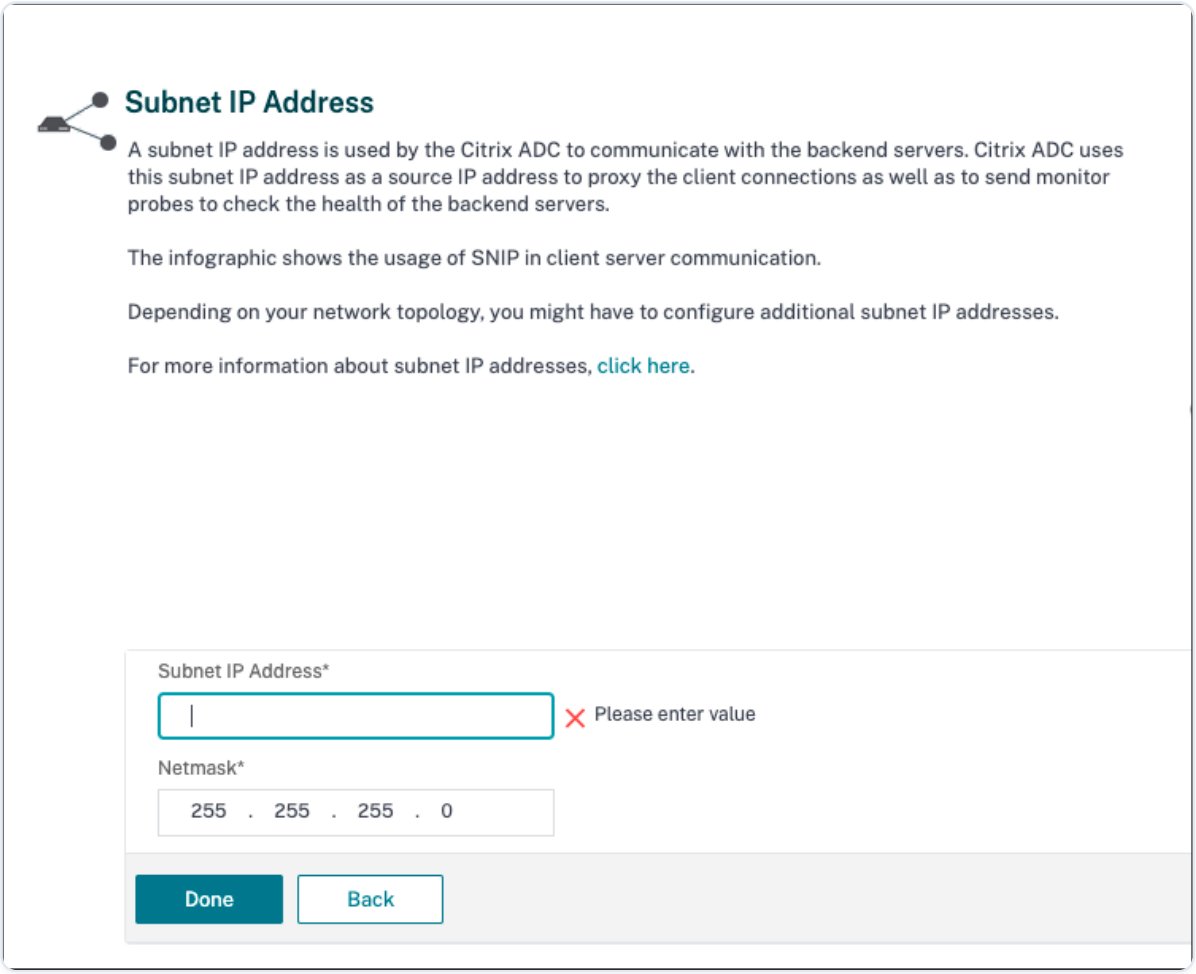
**Nota:**

A configuração desse recurso para o Citrix ADC não é necessária, a menos que você use o Citrix ADC como seu gateway. Se você usa o Citrix ADC, siga estas etapas:

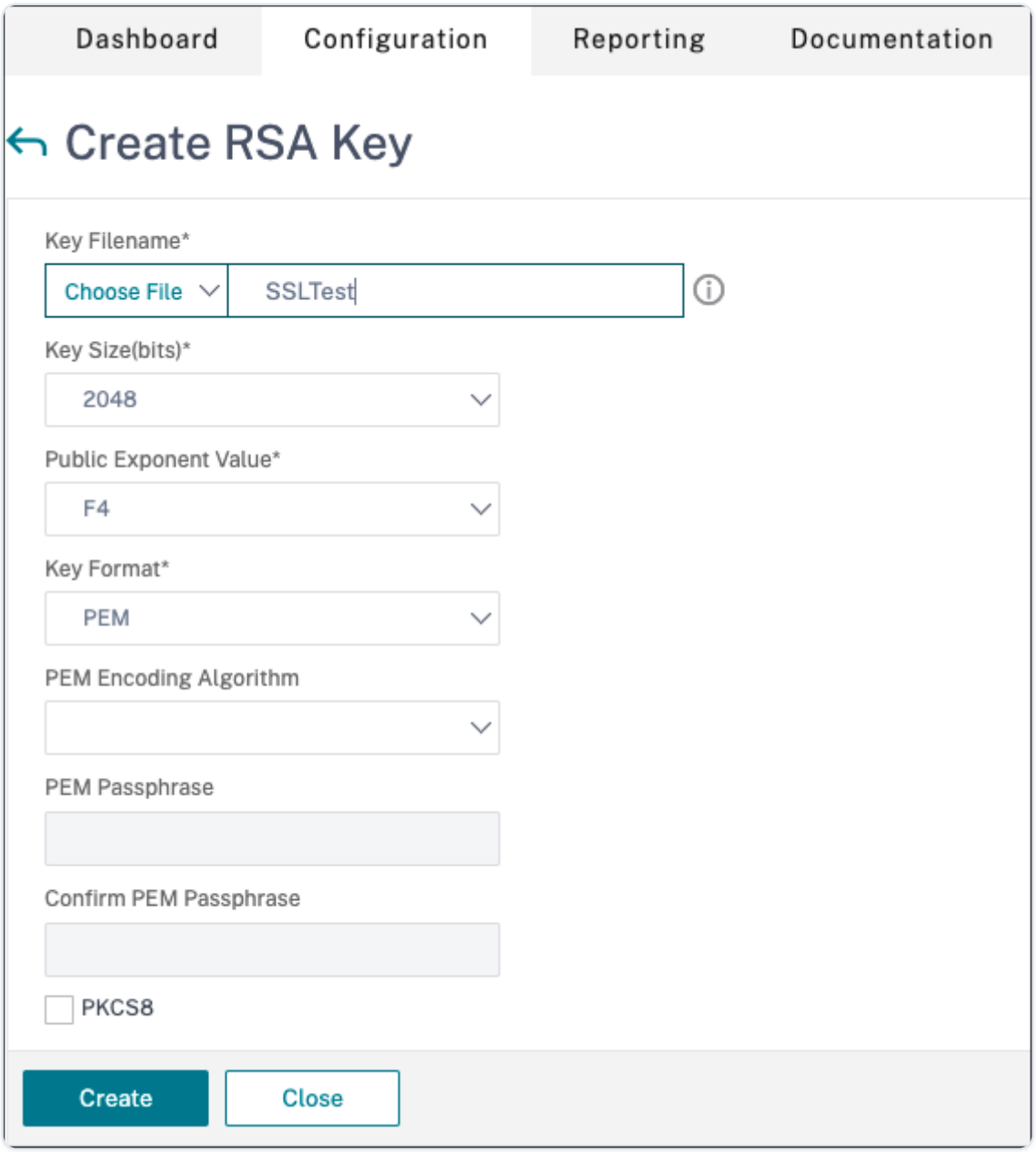
1. Certifique-se de que a seguinte configuração de pré-requisito já esteja em vigor:
    - Os seguintes endereços IP relacionados ao Citrix ADC estão configurados.
        - Endereço IP de Gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



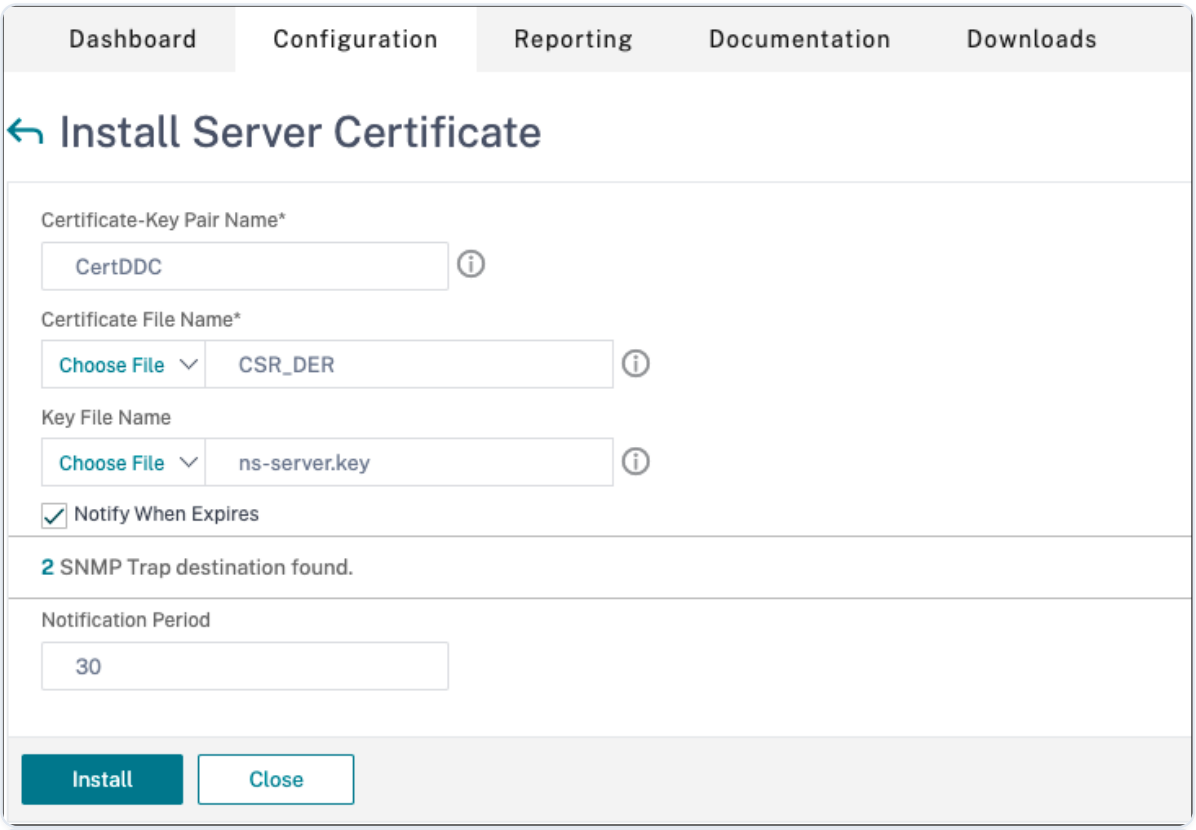

- Endereço IP de sub-rede (SNIP) para habilitar a comunicação entre o dispositivo Citrix ADC e os servidores de back-end. Para obter detalhes, consulte Configuring Subnet IP Addresses.
- Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no dispositivo ADC para o lançamento da sessão. Para obter detalhes, consulte Create a virtual server.

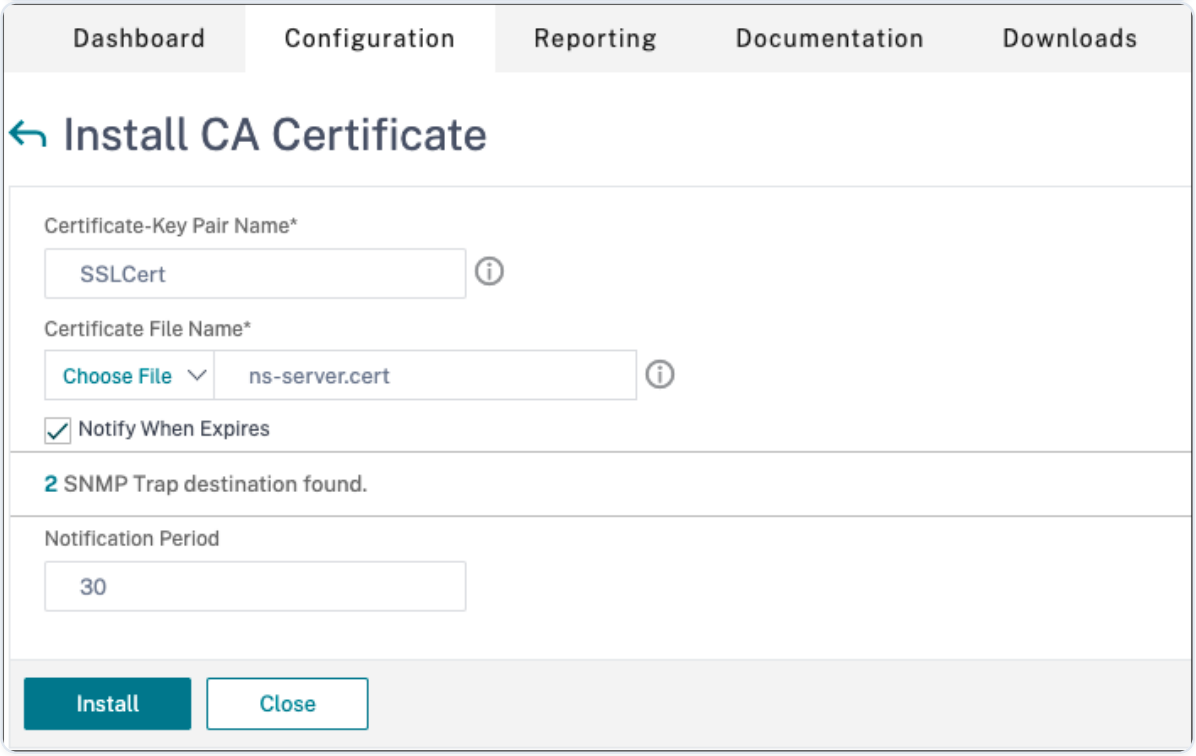



- Os modos e recursos necessários no dispositivo Citrix ADC estão habilitados.
  - Para habilitar os modos, na GUI do Citrix ADC, vá para **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, vá para **System > Settings > Configure Basic Features**.
- As configurações relacionadas a certificados estão concluídas.
  - A Solicitação de Assinatura de Certificado (CSR) é criada. Para obter detalhes, consulte Create a certificate.

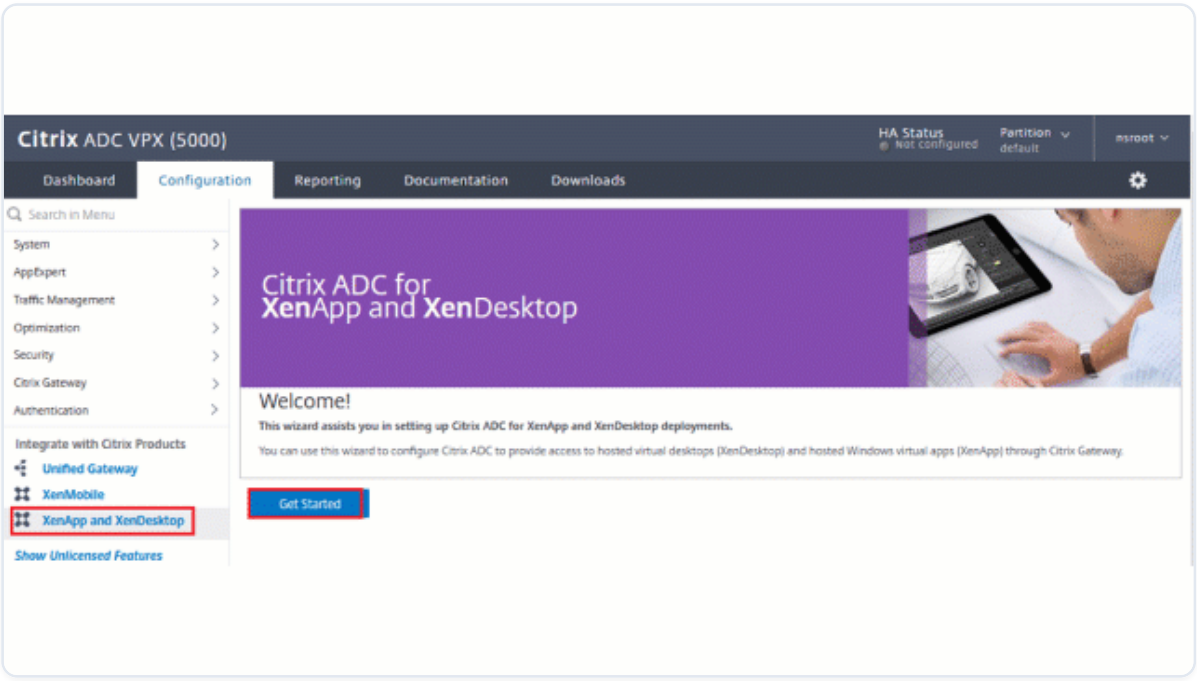



- Os certificados de servidor e CA e os certificados raiz são instalados. Para obter detalhes, consulte Install, link, and updates.



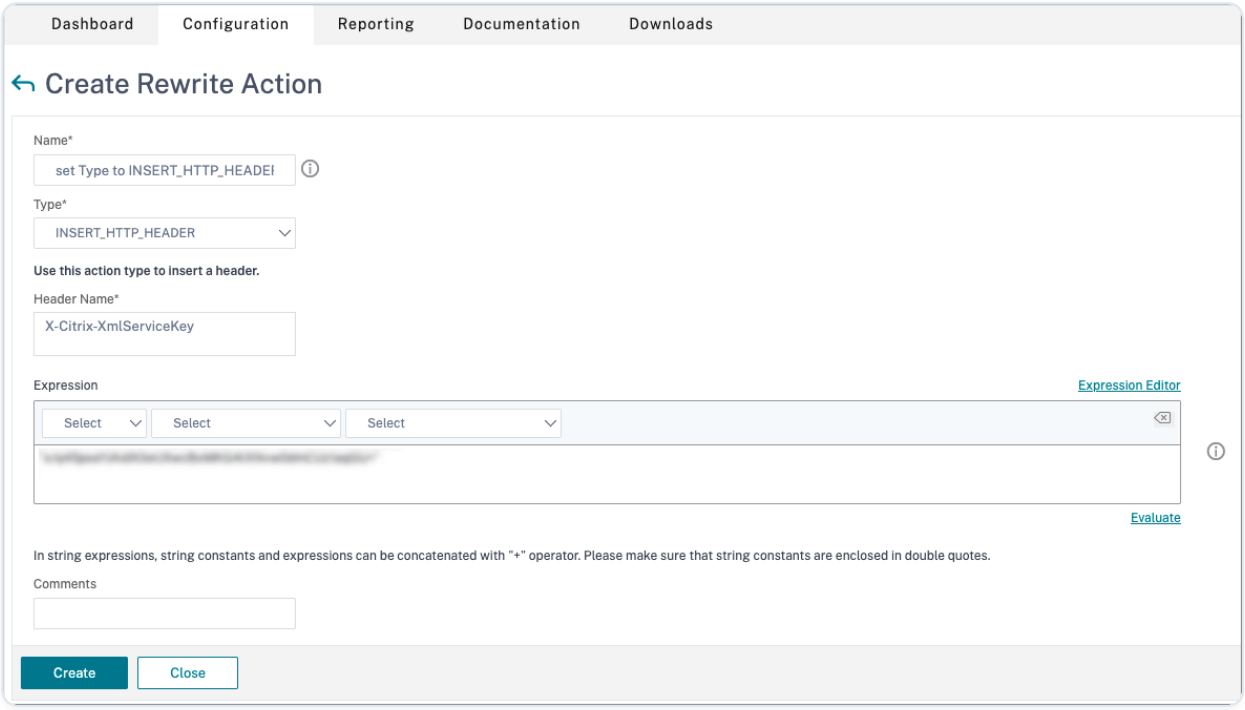

- Um Citrix Gateway foi criado para o Citrix Virtual Desktops. Teste a conectividade clicando no botão **Test STA Connectivity** para confirmar que os servidores virtuais estão online. Para obter detalhes, consulte Configurando o Citrix ADC para Citrix Virtual Apps and Desktops.




2. Adicione uma ação de reescrita. Para obter detalhes, consulte Configuring a Rewrite Action.

   a. Vá para **AppExpert > Rewrite > Actions**.

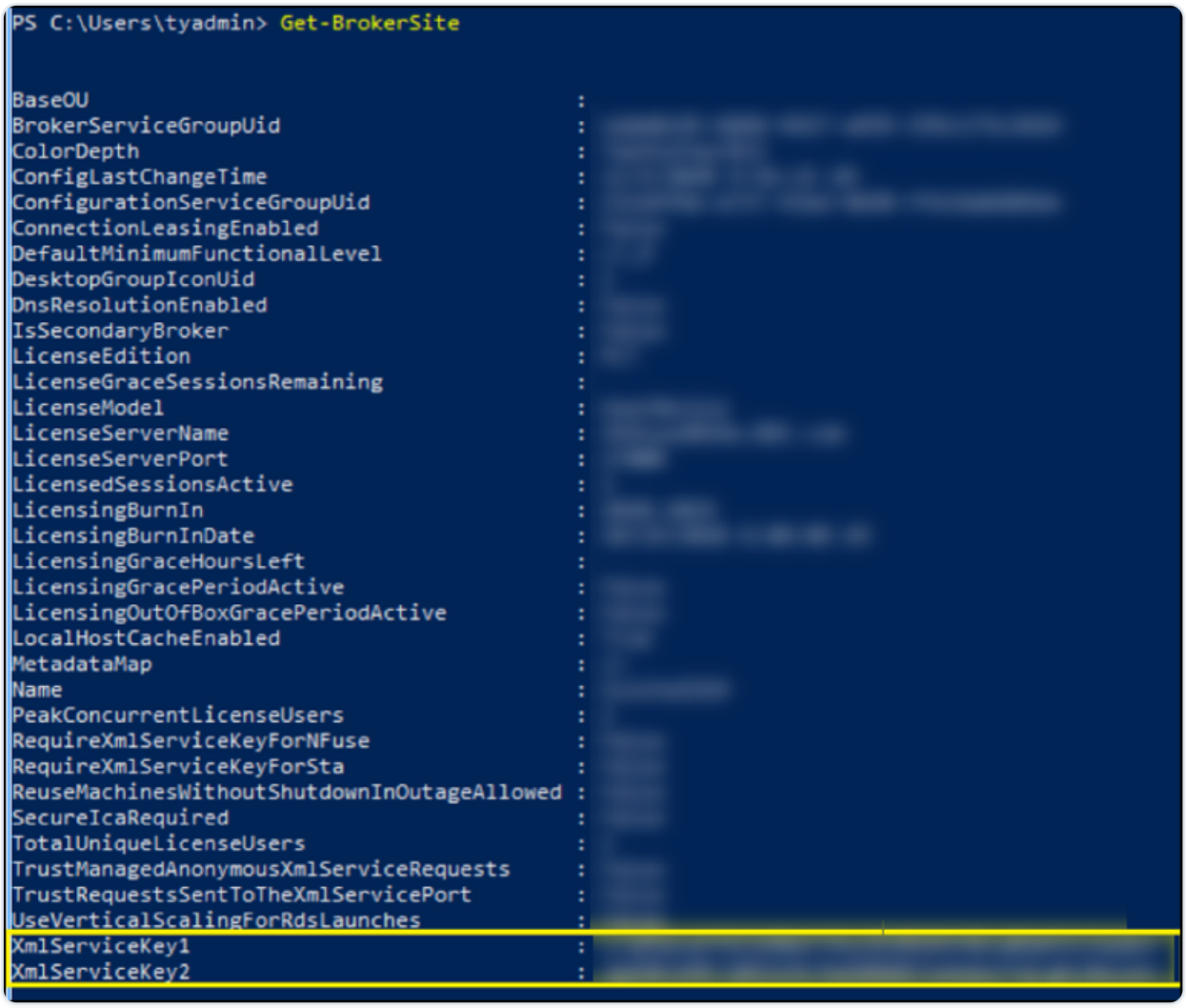
   b. Clique em **Adicionar** para adicionar uma nova ação de reescrita. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".




   a. Em **Tipo**, selecione **INSERT_HTTP_HEADER**.

   b. Em **Nome do Cabeçalho**, insira X-Citrix-XmlServiceKey.

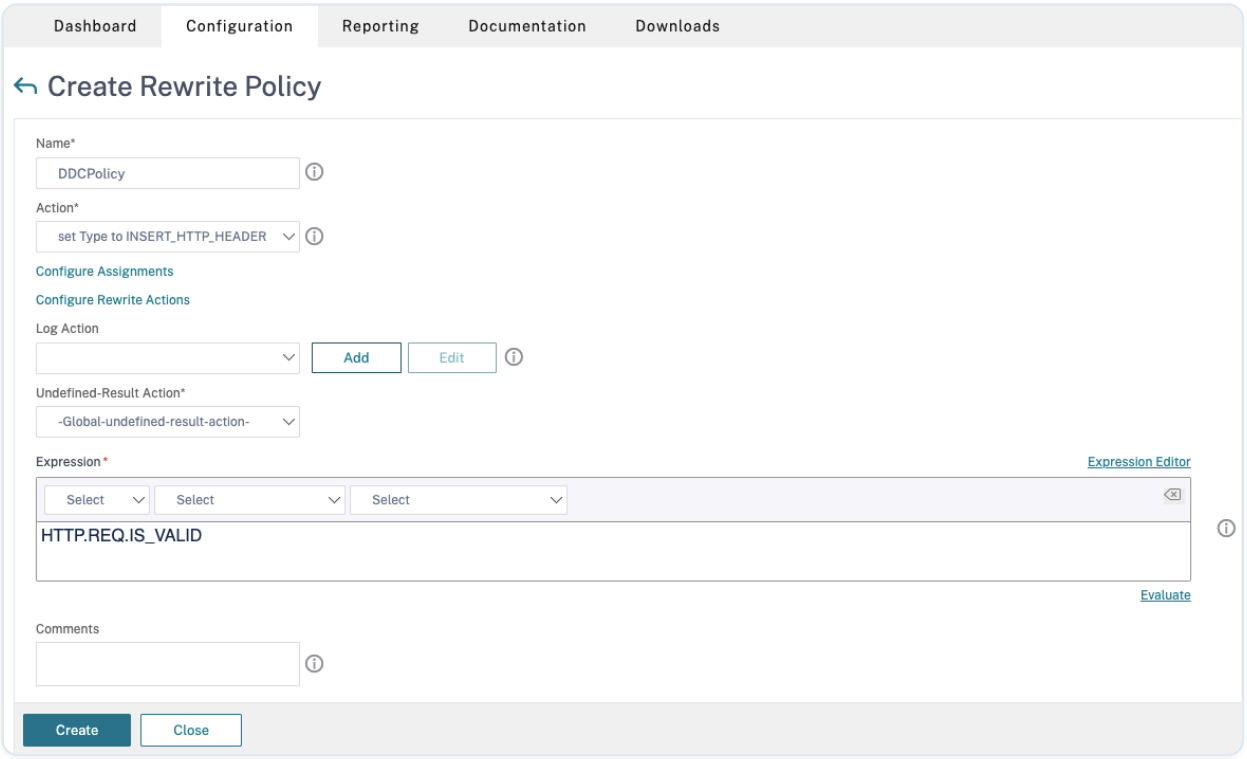
   c. Em **Expressão**, adicione `<XmlServiceKey1 value>` com as aspas. Você pode copiar o valor XmlServiceKey1 da sua configuração do Desktop Delivery Controller™.




3. Adicione uma política de reescrita. Para obter detalhes, consulte Configurando uma Política de Reescrita.

   a. Vá para **AppExpert > Rewrite > Policies**.

   b. Clique em **Adicionar** para adicionar uma nova política.




a. Em **Ação**, selecione a ação criada na etapa anterior.

b. Em **Expressão**, adicione HTTP.REQ.IS_VALID.

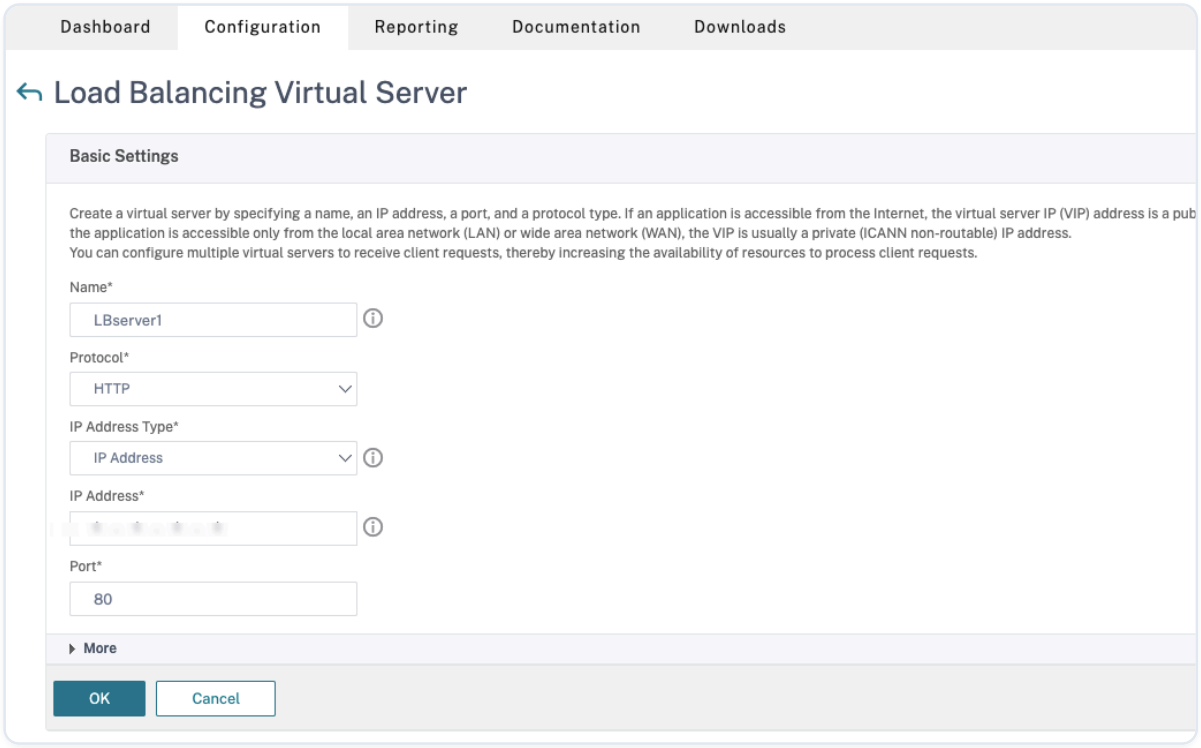
c. Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões falharão ao iniciar.

   Para obter detalhes, consulte Configurar balanceamento de carga básico.

   a. Crie um servidor virtual de balanceamento de carga.

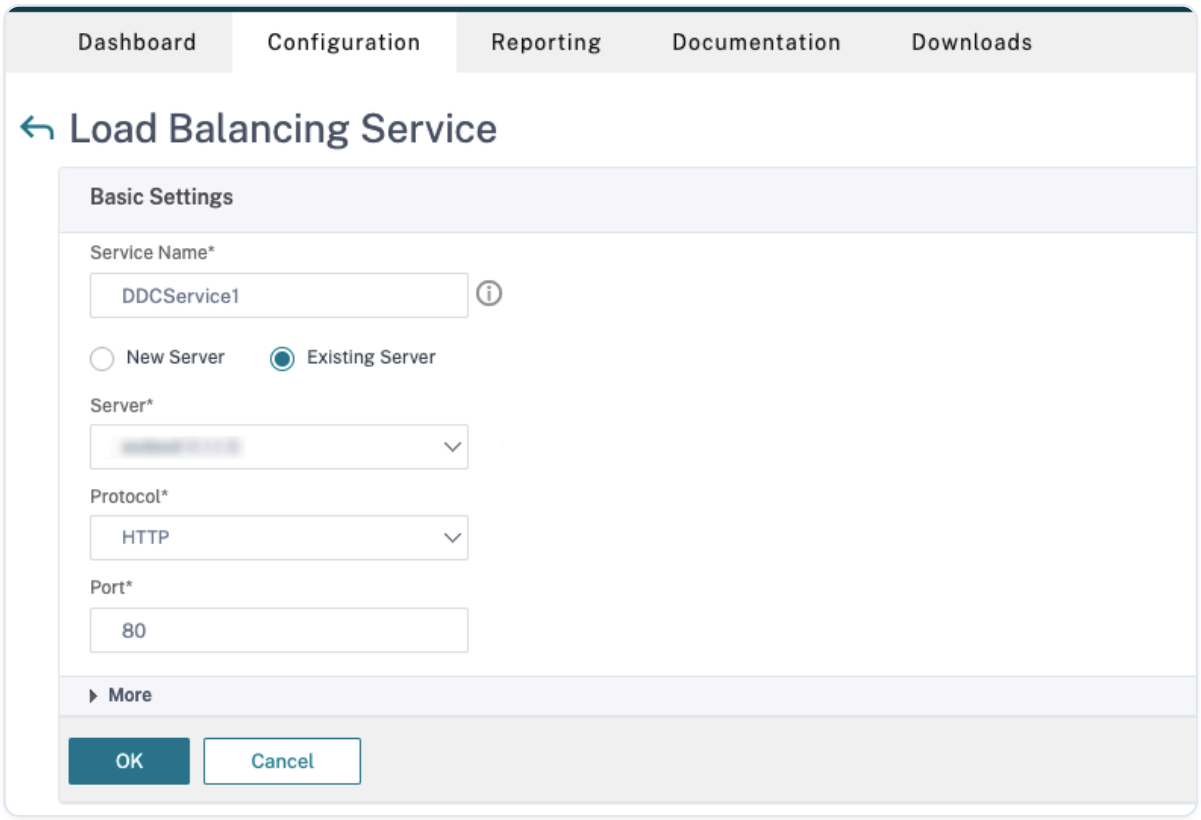
      - Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**.
      - Na página **Servidores Virtuais**, clique em **Adicionar**.




- Em **Protocolo**, selecione **HTTP**.
- Adicione o endereço IP virtual de balanceamento de carga e em **Porta** selecione **80**.
- Clique em **OK**.

b. Crie um serviço de balanceamento de carga.

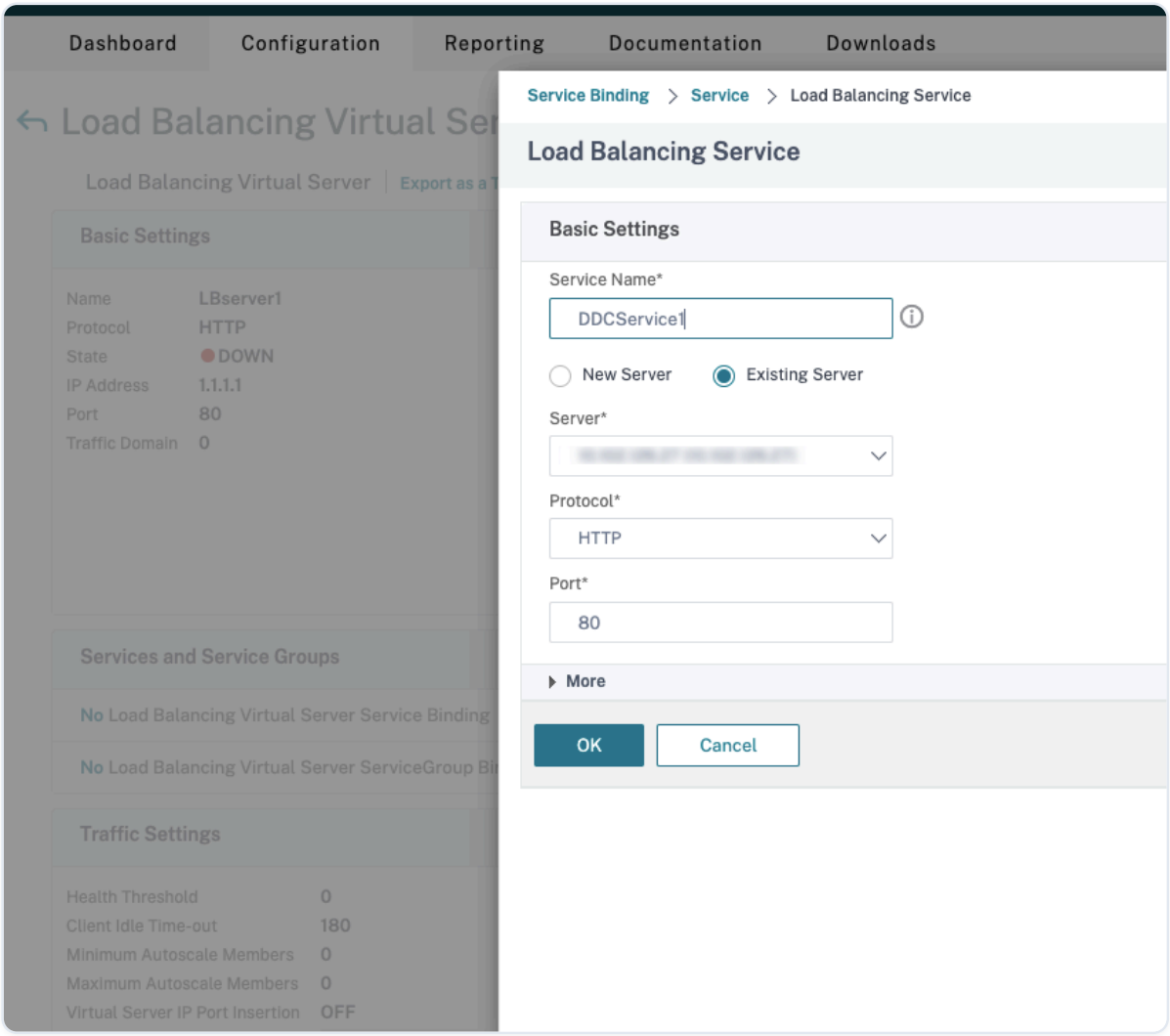
- Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Serviços**.



- Em **Servidor Existente**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocolo**, selecione **HTTP** e em **Porta** selecione **80**.
- Clique em **OK** e, em seguida, clique em **Concluído**.

c. Vincule o serviço ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Serviços e Grupos de Serviço**, clique em **Nenhuma Vinculação de Serviço de Servidor Virtual de Balanceamento de Carga**.

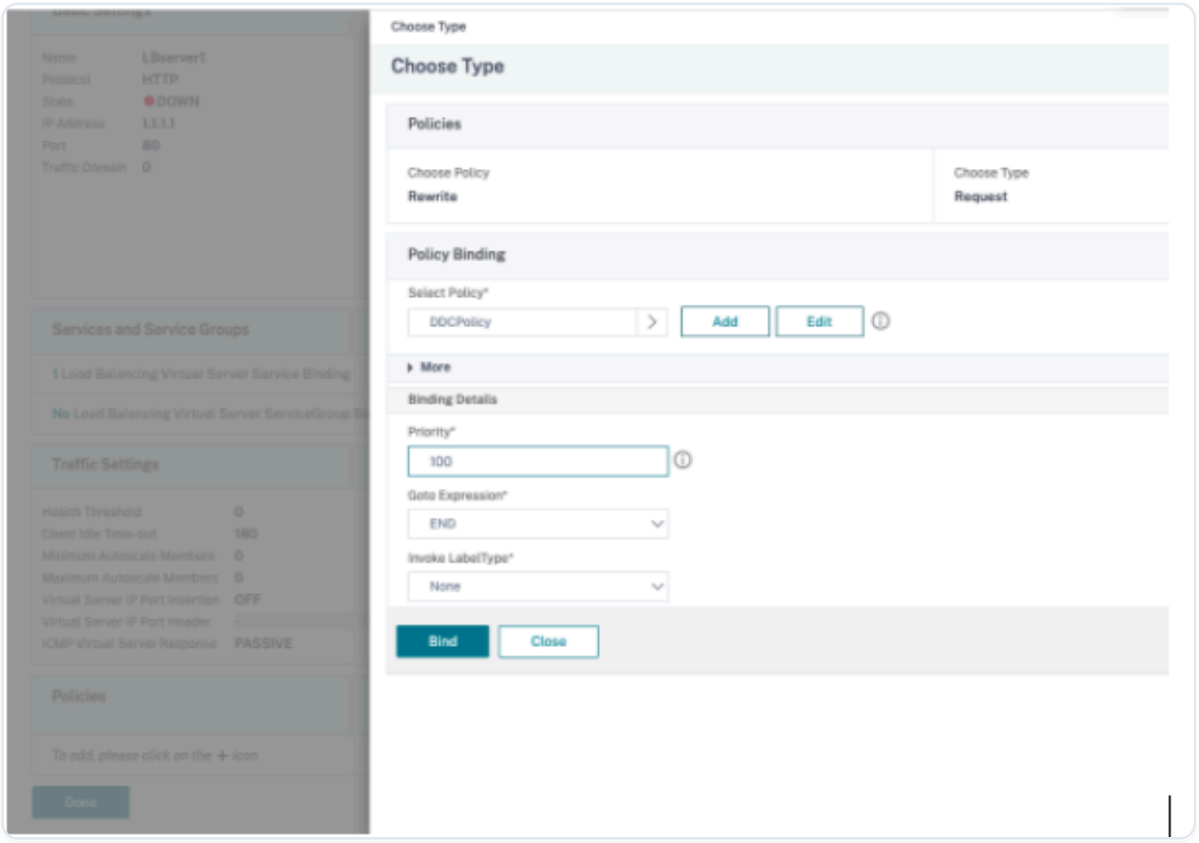



- Em **Service Binding**, selecione o serviço criado anteriormente.
- Clique em **Vincular**.

d. Vincule a política de reescrita criada anteriormente ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.

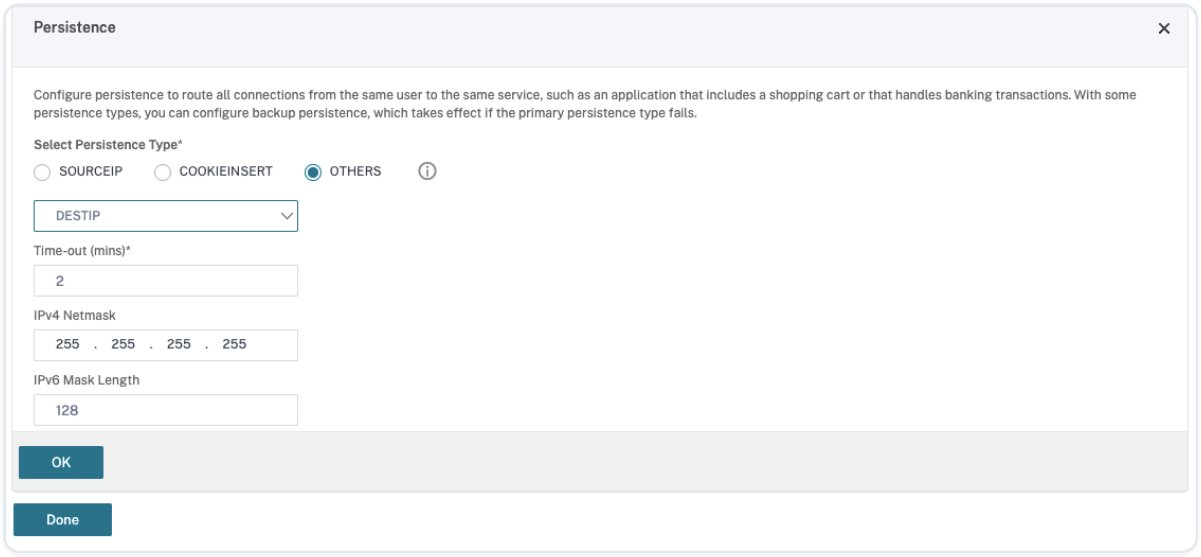
- Em **Configurações Avançadas**, clique em **Políticas,** e, em seguida, na seção **Políticas**, clique em **+**.




- Em **Escolher Política**, selecione **Reescrever** e em **Escolher Tipo**, selecione **Solicitação**.
- Clique em **Continuar**.
- Em **Selecionar Política**, selecione a política de reescrita criada anteriormente.
- Clique em **Vincular**.
- Clique em **Concluído**.

e. Configure a persistência para o servidor virtual, se necessário.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Configurações Avançadas**, clique em **Persistência**.




- Selecione o tipo de persistência como **Outros**.
- Selecione **DESTIP** para criar sessões de persistência com base no endereço IP do serviço selecionado pelo servidor virtual (o endereço IP de destino)
- Em **Máscara de Rede IPv4**, adicione a máscara de rede igual à do DDC.
- Clique em **OK**.

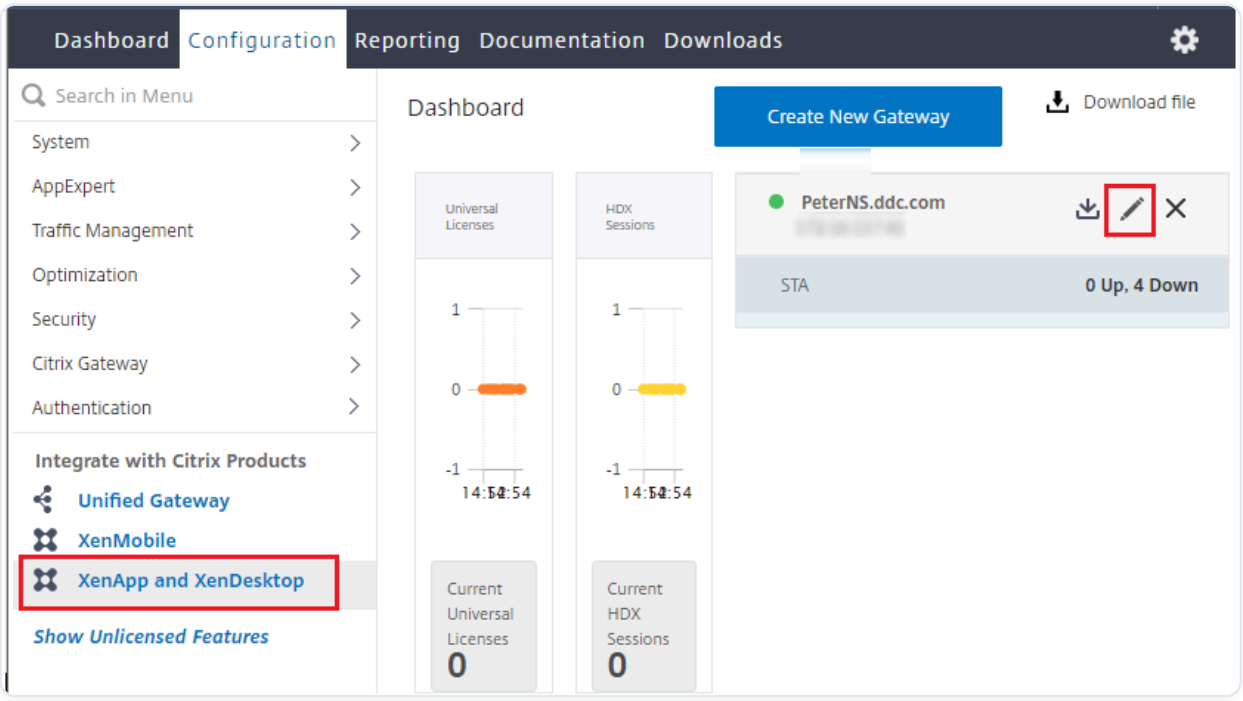
f. Repita estas etapas para o outro servidor virtual também.

### Alterações de configuração se o dispositivo Citrix ADC já estiver configurado com Citrix Virtual Desktops™

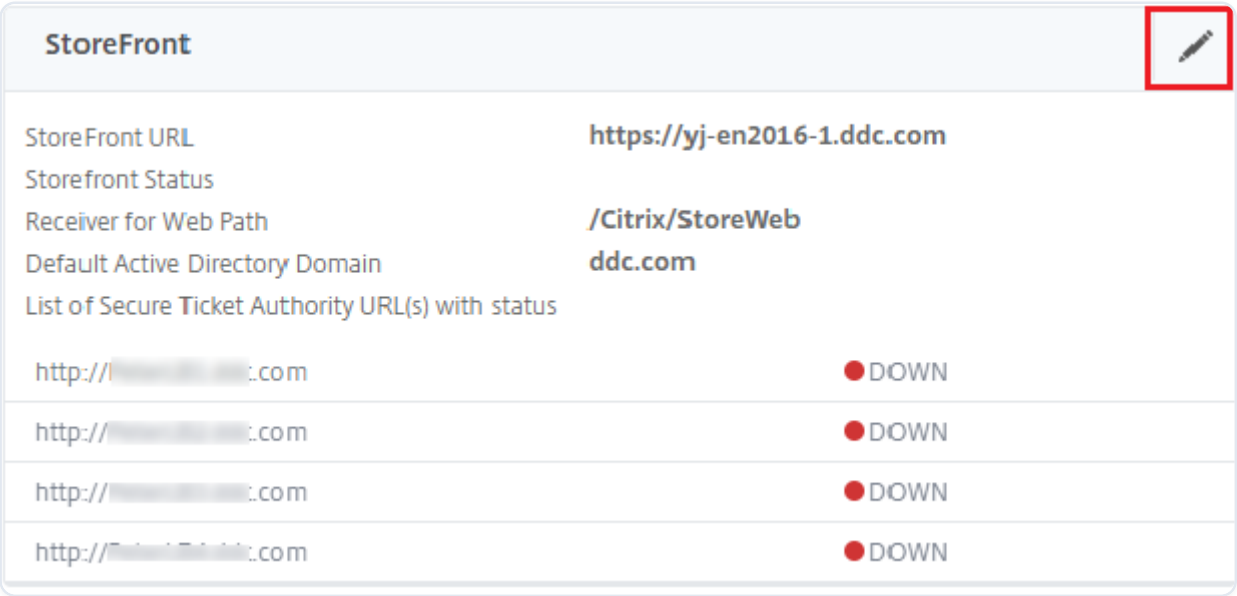
Se você já configurou o dispositivo Citrix ADC com Citrix Virtual Desktops, para usar o recurso Secure XML, você deve fazer as seguintes alterações de configuração.

- Antes do lançamento da sessão, altere a **URL da Autoridade de Ticket de Segurança** do gateway para usar os FQDNs dos servidores virtuais de balanceamento de carga.
- Certifique-se de que o parâmetro `TrustRequestsSentToTheXmlServicePort` esteja definido como False. Por padrão, o parâmetro `TrustRequestsSentToTheXmlServicePort` é definido como False. No entanto, se o cliente já configurou o Citrix ADC para o Citrix Virtual Desktops, então o `TrustRequestsSentToTheXmlServicePort` é definido como True.

1. Na GUI do Citrix ADC, vá para **Configuração > Integrar com Produtos Citrix** e clique em **XenApp and XenDesktop®**.
2. Selecione a instância do gateway e clique no ícone de edição.

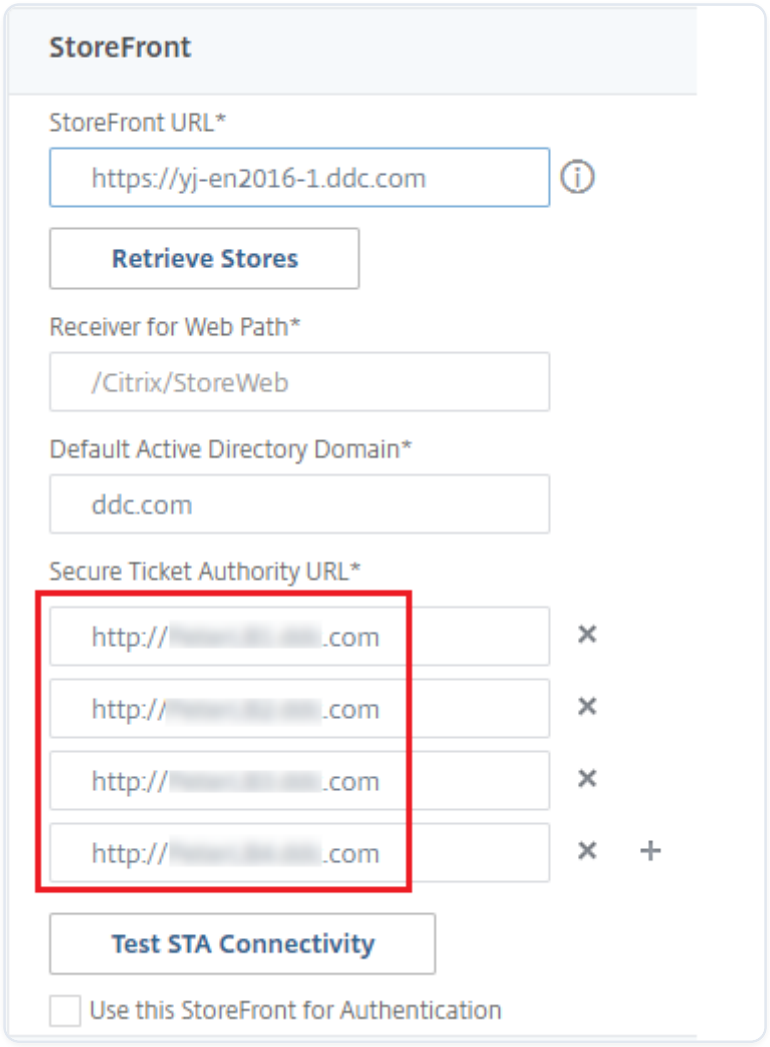



3. No painel StoreFront, clique no ícone de edição.




4. Adicione a **URL da Secure Ticket Authority**.

   - Se o recurso Secure XML estiver ativado, a URL do STA deve ser a URL do serviço de balanceamento de carga.
   - Se o recurso Secure XML estiver desativado, a URL do STA deve ser a URL do STA (endereço do DDC) e o parâmetro TrustRequestsSentToTheXmlServicePort no DDC deve ser definido como True.




# Configurações de resiliência de sessão

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência ao usuário. A perda de conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode levar à frustração do usuário. Mover-se rapidamente entre dispositivos e acessar os mesmos aplicativos a cada logon é uma prioridade para muitos trabalhadores móveis, como profissionais de saúde.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões, reduzem inconvenientes, tempo de inatividade e perda de produtividade; usando esses recursos, os usuários móveis podem se mover de forma rápida e fácil entre dispositivos.

## Confiabilidade da sessão

A Confiabilidade da Sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Esse recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel ferroviário e perde momentaneamente a conectividade. Normalmente, a sessão é desconectada e desaparece da tela do usuário, e o usuário precisa se reconectar à sessão desconectada. Com a Confiabilidade da Sessão, a sessão permanece ativa na máquina. Para indicar a perda de conectividade, a tela do usuário congela e o cursor muda para uma ampulheta giratória até que a conectividade seja retomada do outro lado do túnel. O usuário continua a acessar a tela durante a interrupção e pode retomar a interação com o aplicativo quando a conexão de rede é restaurada. A Confiabilidade da Sessão reconecta os usuários sem solicitações de reautenticação.

Os usuários do aplicativo Citrix Workspace™ não podem substituir a configuração do Controller.

Você pode usar a Confiabilidade da Sessão com o Transport Layer Security (TLS). O TLS criptografa apenas os dados enviados entre o dispositivo do usuário e o Citrix Gateway.

Habilite e configure a Confiabilidade da Sessão com as seguintes configurações de política:

- A configuração de política de conexões de confiabilidade da sessão permite ou impede a confiabilidade da sessão.
- A configuração de política de tempo limite de confiabilidade da sessão tem um padrão de 180 segundos, ou três minutos. Embora você possa estender o tempo que a confiabilidade da sessão mantém uma sessão aberta, esse recurso foi projetado para a conveniência do usuário. Portanto, ele não solicita reautenticação ao usuário. À medida que você estende o tempo em que uma sessão é mantida aberta, aumentam as chances de um usuário se distrair e se afastar do dispositivo do usuário. Essas ações podem potencialmente deixar a sessão acessível a usuários não autorizados.
- As conexões de confiabilidade de sessão de entrada usam a porta 2598, a menos que você altere o número da porta na configuração de política de número da porta de confiabilidade da sessão.
- Para evitar que os usuários se reconectem a sessões interrompidas sem precisar se reautenticar, use o recurso Auto Client Reconnect. Você pode configurar a configuração de política de autenticação do Auto Client Reconnect para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usar a Confiabilidade da Sessão e o Auto Client Reconnect, os dois recursos funcionarão em sequência. A Confiabilidade da Sessão fecha, ou desconecta, a sessão do usuário após o tempo especificado na configuração de política de tempo limite de confiabilidade da sessão. Depois disso, as configurações de política do Auto Client Reconnect entram em vigor, tentando reconectar o usuário à sessão desconectada.

## Reconexão Automática do Cliente

Com o recurso Auto Client Reconnect, o Citrix Workspace app pode detectar desconexões não intencionais de sessões ICA® e reconectar os usuários às sessões afetadas automaticamente. Quando este recurso está ativado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Para sessões de aplicativo, o Citrix Workspace app tenta se reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de desktop, o Citrix Workspace app tenta se reconectar à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, este período é de cinco minutos. Para alterar este período, edite a seguinte configuração de registro no dispositivo do usuário (onde `seconds` é o número de segundos após o qual não são feitas mais tentativas de reconectar a sessão).

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

Habilite e configure o Auto Client Reconnect com as seguintes configurações de política:

- **Auto Client Reconnect:** Habilita ou desabilita a reconexão automática pelo Citrix Workspace app após uma conexão ter sido interrompida.
- **Autenticação de Auto Client Reconnect:** Habilita ou desabilita a exigência de autenticação do usuário após a reconexão automática.
- **Registro de Auto Client Reconnect:** Habilita ou desabilita o registro de eventos de reconexão no log de eventos. O registro é desabilitado por padrão. Quando habilitado, o log do sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Cada servidor armazena informações sobre eventos de reconexão em seu próprio log do sistema. O site não fornece um log combinado de eventos de reconexão para todos os servidores.

> **Observação:**
>
> O Auto Client Reconnect sem reautenticação é suportado apenas para autenticação por senha. Se você usar o Federated Authentication Service ou a autenticação por cartão inteligente, o Auto Client Reconnect sem reautenticação não é suportado. Nesses casos, os usuários são redirecionados para a tela de login.

> O Auto Client Reconnect incorpora um mecanismo de autenticação baseado em credenciais de usuário criptografadas. Quando um usuário faz login inicialmente, o servidor criptografa e armazena as credenciais do usuário na memória. O servidor também cria e envia um cookie contendo a chave de criptografia para o Citrix Workspace app. O Citrix Workspace app envia a chave para o servidor para reconexão. O servidor descriptografa as credenciais e as envia para o logon do Windows para autenticação. Quando os cookies expiram, os usuários devem se reautenticar para se reconectar às sessões.

Os cookies não são usados se você habilitar a configuração de autenticação do Auto Client Reconnect. Em vez disso, os usuários são apresentados a uma caixa de diálogo solicitando credenciais quando o Citrix Workspace app tenta se reconectar automaticamente.

Para proteção máxima das credenciais e sessões do usuário, use criptografia para toda a comunicação entre clientes e o site.

Desabilite o Auto Client Reconnect no Citrix Workspace app para Windows usando o arquivo icaclient.adm. Para obter mais informações, consulte a documentação da sua versão do Citrix Workspace app para Windows.

As configurações para conexões também afetam o Auto Client Reconnect:

- Por padrão, o Auto Client Reconnect é habilitado por meio de configurações de política no nível do site, conforme descrito anteriormente. A reautenticação do usuário não é necessária. No entanto, se a conexão ICA TCP de um servidor estiver configurada para redefinir sessões com um link de comunicação interrompido, a reconexão automática não ocorrerá. O Auto Client Reconnect funciona apenas se o servidor desconectar as sessões quando houver uma conexão interrompida ou com tempo limite. Neste contexto, a conexão ICA TCP refere-se a uma porta virtual de um servidor (em vez de uma conexão de rede real) que é usada para sessões em redes TCP/IP.
- Por padrão, a conexão ICA TCP em um servidor é configurada para desconectar sessões com conexões interrompidas ou com tempo limite. As sessões desconectadas permanecem intactas na memória do sistema e estão disponíveis para reconexão pelo Citrix Workspace app.
- A conexão pode ser configurada para redefinir ou desconectar sessões com conexões quebradas ou com tempo limite. Quando uma sessão é redefinida, a tentativa de reconectar inicia uma nova sessão. Em vez de restaurar um usuário para o mesmo local no aplicativo em uso, o aplicativo é reiniciado.

- Se o servidor estiver configurado para redefinir sessões, o Auto Client Reconnect criará uma nova sessão. Esse processo exige que os usuários insiram suas credenciais para fazer logon no servidor.
- A reconexão automática pode falhar se o aplicativo Citrix Workspace ou o plug-in enviar informações de autenticação incorretas, o que pode ocorrer durante um ataque ou se o servidor determinar que muito tempo se passou desde que detectou a conexão quebrada.

## ICA Keep-Alive

A ativação do recurso ICA Keep-Alive impede que conexões quebradas sejam desconectadas. Quando ativado, se o servidor não detectar atividade, esse recurso impede que os Serviços de Área de Trabalho Remota desconectem essa sessão. Exemplos de nenhuma atividade incluem nenhuma alteração de relógio, nenhum movimento do mouse, nenhuma atualização de tela. O servidor envia pacotes keep-alive a cada poucos segundos para detectar se a sessão está ativa. Se a sessão não estiver mais ativa, o servidor a marca como desconectada.

> **Importante:**
>
> O ICA Keep-Alive funciona somente se você não estiver usando a Confiabilidade da Sessão. A Confiabilidade da Sessão tem seus próprios mecanismos para evitar que conexões quebradas sejam desconectadas. Configure o ICA Keep-Alive apenas para conexões que não usam a Confiabilidade da Sessão.

> As configurações do ICA Keep-Alive substituem as configurações de keep-alive configuradas na Política de Grupo do Windows.

Habilite e configure o ICA Keep-Alive com as seguintes configurações de política:

- **Tempo limite de keep-alive do ICA:** Especifica o intervalo (1-3600 segundos) usado para enviar mensagens keep-alive do ICA. Não configure esta opção se você quiser que seu software de monitoramento de rede feche conexões inativas em ambientes onde as conexões quebradas são tão infrequentes que permitir que os usuários se reconectem às sessões não é uma preocupação.

  O intervalo padrão é de 60 segundos: pacotes ICA Keep-Alive são enviados para os dispositivos do usuário a cada 60 segundos. Se um dispositivo de usuário não responder em 60 segundos, o status das sessões ICA muda para desconectado.
- **Keep-alives do ICA:** Envia ou impede o envio de mensagens keep-alive do ICA.

## Controle de workspace

O controle de workspace permite que desktops e aplicativos sigam um usuário de um dispositivo para outro. Essa capacidade de roaming permite que um usuário acesse todos os desktops ou aplicativos abertos de qualquer lugar simplesmente fazendo logon, sem precisar reiniciar os desktops ou aplicativos em cada dispositivo. Por exemplo, o controle de workspace pode ajudar profissionais de saúde em um hospital que precisam se mover rapidamente entre diferentes estações de trabalho e acessar o mesmo conjunto de aplicativos cada vez que fazem logon. Se você configurar as opções de controle de workspace para permitir, esses trabalhadores podem se desconectar de vários aplicativos em um dispositivo cliente e, em seguida, reconectar-se para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle de workspace afeta as seguintes atividades:

- **Logon:** Por padrão, o controle de workspace permite que os usuários se reconectem automaticamente a todos os desktops e aplicativos em execução ao fazer logon, eliminando a necessidade de reabri-los manualmente. Através do controle de workspace, os usuários podem abrir desktops ou aplicativos desconectados, além de quaisquer que estejam ativos em outro dispositivo cliente. Desconectar-se de um desktop ou aplicativo o deixa em execução no servidor. Se você tiver usuários em roaming que precisam manter alguns desktops ou aplicativos em execução em um dispositivo cliente enquanto se reconectam a um subconjunto de seus desktops ou aplicativos em outro dispositivo cliente, você pode configurar o comportamento de reconexão de logon para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Reconectando:** Após fazer logon no servidor, os usuários podem se reconectar a todos os seus desktops ou aplicativos a qualquer momento clicando em Reconectar. Por padrão, Reconectar abre desktops ou aplicativos que estão desconectados, além de quaisquer outros que estejam atualmente em execução em outro dispositivo cliente. Você pode configurar Reconectar para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Fazendo logoff:** Para usuários que abrem desktops ou aplicativos através do StoreFront™, você pode configurar o comando **Log Off** para desconectar o usuário do StoreFront e de todas as sessões ativas, ou apenas do StoreFront.
- **Desconectando:** Os usuários podem se desconectar de todos os desktops e aplicativos em execução de uma só vez, sem a necessidade de se desconectar de cada um individualmente.

O controle de espaço de trabalho está disponível apenas para usuários do Citrix Workspace app que acessam desktops e aplicativos por meio de uma conexão Citrix StoreFront. Por padrão, o controle de espaço de trabalho é desabilitado para sessões de desktop virtual, mas é habilitado

para aplicativos hospedados. O compartilhamento de sessão não ocorre por padrão entre desktops publicados e quaisquer aplicativos publicados em execução dentro desses desktops.

As políticas de usuário, mapeamentos de unidade cliente e configurações de impressora mudam apropriadamente quando um usuário se move para um novo dispositivo cliente. As políticas e mapeamentos são aplicados de acordo com o dispositivo cliente onde o usuário está logado na sessão. Por exemplo, um profissional de saúde faz logoff de um dispositivo na sala de emergência e, em seguida, faz logon em uma estação de trabalho no laboratório de raios-X. As políticas, mapeamentos de impressora e mapeamentos de unidade cliente apropriados para a sessão no laboratório de raios-X entram em vigor no início da sessão.

Você pode personalizar quais impressoras aparecem para os usuários quando eles mudam de local. Você também pode controlar se os usuários podem imprimir em impressoras locais, quanta largura de banda é consumida quando os usuários se conectam remotamente e outros aspectos de suas experiências de impressão.

Para obter informações sobre como habilitar e configurar o controle de espaço de trabalho para usuários, consulte a documentação do StoreFront.

## Roaming de sessão

> **Observação:**

> As informações a seguir o guiam para configurar o roaming de sessão usando o PowerShell. Você pode usar o Web Studio em vez disso. Para obter mais informações, consulte (/pt-br/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-manage.html#configure-session-roaming).

> Por padrão, as sessões fazem roaming entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos estão disponíveis em ambos os dispositivos. Os aplicativos seguem, independentemente do dispositivo ou se existem sessões atuais. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem.

Embora esse comportamento padrão ofereça muitas vantagens, ele pode não ser ideal em todos os casos. Você pode impedir o roaming de sessão usando o PowerShell SDK.

Exemplo 1: Um profissional de saúde está usando dois dispositivos, preenchendo um formulário de seguro em um PC desktop e consultando informações do paciente em um tablet.

- Se o roaming de sessão estiver habilitado, ambos os aplicativos aparecem em ambos os dispositivos (um aplicativo iniciado em um dispositivo é visível em todos os dispositivos em uso). Isso pode não atender aos requisitos de segurança.
- Se o roaming de sessão estiver desabilitado, o registro do paciente não aparece no PC desktop, e o formulário de seguro não aparece no tablet.

Exemplo 2: Um gerente de produção inicia um aplicativo no PC em seu escritório. O nome e a localização do dispositivo determinam quais impressoras e outros recursos estão disponíveis para essa sessão. Mais tarde no dia, ele vai a um escritório no prédio ao lado para uma reunião que exigirá o uso de uma impressora.

- Quando o roaming de sessão está ativado, o gerente de produção provavelmente não conseguiria acessar as impressoras perto da sala de reunião, porque os aplicativos que ele iniciou anteriormente em seu escritório resultaram na atribuição de impressoras e outros recursos perto daquele local.
- Quando o roaming de sessão está desativado, ao fazer logon em uma máquina diferente (usando as mesmas credenciais), uma nova sessão é iniciada, e impressoras e recursos próximos estarão disponíveis.

### Configurar o roaming de sessão

Para configurar o roaming de sessão, use os seguintes cmdlets de regra de política de direito com a propriedade "SessionReconnection". Opcionalmente, você também pode especificar a propriedade "LeasingBehavior".

Para sessões de desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões de aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Always:** As sessões sempre fazem roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.

- **DisconnectedOnly:** Reconectar apenas a sessões que já estão desconectadas; caso contrário, iniciar uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente, primeiro desconectando-os ou usando o Workspace Control para fazer o roaming explicitamente.) Uma sessão ativa conectada de outro dispositivo cliente nunca é usada. Em vez disso, uma nova sessão é iniciada.
- **SameEndpointOnly:** Um usuário obtém uma sessão exclusiva para cada dispositivo cliente que usa. Isso desativa completamente o roaming. Os usuários podem se reconectar apenas ao mesmo dispositivo que foi usado anteriormente na sessão.

A propriedade "LeasingBehavior" é descrita abaixo.

**Efeitos de outras configurações:**

A desativação do roaming de sessão é afetada pelo limite de aplicativo **Permitir apenas uma instância do aplicativo por usuário** nas propriedades do aplicativo no grupo de entrega.

- Se você desativar o roaming de sessão, desative o limite de aplicativo "Permitir apenas uma instância ...".
- Se você ativar o limite de aplicativo "Permitir apenas uma instância ...", não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos.

## Intervalo de logon

Se uma máquina virtual contendo um VDA de desktop for encerrada antes que o processo de logon seja concluído, você pode alocar mais tempo para o processo. O padrão para a versão 7.6 e posteriores é de 180 segundos (o padrão para 7.0-7.5 é de 90 segundos).

Na máquina (ou na imagem mestre usada em um catálogo de máquinas), defina a seguinte chave de registro:

Chave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique um tempo decimal em segundos, no intervalo de 0 a 3600.

Se você alterar uma imagem mestre, atualize o catálogo.

Essa configuração se aplica apenas a VMs com VDAs de desktop. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor.

# Configurações

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

> Você pode usar o Web Studio para gerenciar estas configurações:

- Gerenciar Autenticação
- Programa de Melhoria da Experiência do Cliente Citrix
- Remover Delivery Controllers
- Alterar o banco de dados de log
- Definir data e hora
- Centralizar o gerenciamento do site
- Habilitar atribuição automática de vários usuários para Acesso Remoto a PC
- Habilitar resolução de DNS
- Habilitar confiança XML
- Gerenciar chave de segurança
- Definir o tempo limite de inatividade para o console do Studio

## Gerenciar autenticação

Por padrão, os usuários fazem logon no Web Studio usando seu nome de usuário e senha de domínio. Você também pode escolher um método de autenticação diferente para os usuários, como a autenticação por cartão inteligente ou a autenticação integrada do Windows.

### Gerenciar usando o Studio

Para escolher um método de autenticação para usuários, siga estas etapas:

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Localize o bloco **Autenticação** e clique em **Editar** para selecionar uma opção:

- **Credenciais de domínio**
- **Credenciais de domínio ou autenticação integrada do Windows**

  Com a autenticação integrada do Windows ativada, os usuários podem acessar o Web Studio usando suas credenciais do Windows (Kerberos/NTLM) ou um certificado de cliente.

  Quando o Web Studio e o Delivery Controller™ são instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, ative o acesso entre origens e adicione o URL do servidor Web Studio à lista de permissões.

  > **Importante**
  >
  > A autenticação integrada do Windows não funciona quando o Web Studio está configurado como um proxy para os Delivery Controllers.

- **Autenticação por cartão inteligente**
- **Credenciais de domínio ou autenticação por cartão inteligente**

  A ativação da autenticação por cartão inteligente requer configuração adicional. Para obter mais informações, consulte Configurar a autenticação por cartão inteligente para o Web Studio.

### Gerenciar usando o script PowerShell

O método de autenticação é configurado no banco de dados do Delivery Controller. Você pode usar o seguinte script PowerShell para definir o método de autenticação:

1. Obtenha o ID do site atual executando o seguinte comando no Delivery Controller:

   ```
   Get-ConfigSite | Select SiteGuid
   ```

2. Defina o método de autenticação executando o seguinte script:

   ```
   # Generate a new bearer token

   $bearerData = New-TrustBearerToken

   # Define the Delivery Controller DNS name and Site ID

   $ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
   ```

```
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1

# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

### Configurar os navegadores para autenticação integrada do Windows

Se você habilitar a *autenticação integrada do Windows* usando **Credenciais de domínio ou autenticação integrada do Windows**, na próxima vez que seus usuários fizerem login, eles serão automaticamente conectados. Como usuário, se você não conseguir fazer login automaticamente, siga estas etapas para configurar seu navegador da web para permitir a autenticação integrada do Windows.

Para o Google Chrome:

1. No Painel de Controle, selecione **Opções da Internet**.
2. Selecione a guia **Avançado**.
3. Selecione **Habilitar Autenticação Integrada do Windows**.
4. Selecione a guia **Segurança**.
5. Selecione **Intranet Local > Sites > Avançado**.
6. Na caixa **Adicionar este site à zona**:
    - Se o Web Studio e o Delivery Controller residirem no mesmo servidor, digite o URL do host que executa o Web Studio.
    - Caso contrário, digite um domínio curinga. Exemplo: se o Delivery Controller estiver em `ddc.domain.com`, digite `*.domain.com`.
7. Clique em **Adicionar > Fechar**

Para o Mozilla Firefox:

1. No navegador, digite `about:config` na caixa de URL.
2. Na caixa **Pesquisar**, digite `network negotiate`.
3. Clique com o botão direito em **network.negotiate-auth.trusted-uris** e selecione **Modificar**.
4. Na caixa **Inserir valor da string**:
    - Se o Web Studio e o Delivery Controller residirem no mesmo servidor, adicione uma lista de URLs e/ou aliases separados por vírgulas, 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 **Logon integrado do Windows** na página de logon para tentar novamente.

Quando o Web Studio e o Delivery Controller são instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, você precisa habilitar **Permitir acesso entre origens**.

Siga estas etapas para habilitar **Permitir acesso entre origens**:

1. Marque a caixa de seleção **Permitir acesso entre origens**.

2. Adicione a URL do servidor Web Studio à lista de permissões.
3. No campo **Inserir URL**, digite a URL. Clique em **Adicionar** para adicionar mais, se necessário.

> **Nota**
>
> - A URL deve seguir o formato correto: `<scheme>://<hostname>`. Certifique-se de que ela não inclua nenhum caminho ou barra final.
> - Endereços IP e FQDNs são suportados. Ao adicionar uma URL, certifique-se de que ela corresponda à forma como você acessa o Web Studio. Por exemplo, se estiver acessando o Web Studio usando um endereço IP, adicione a URL baseada em endereço IP à lista.
> - Se você usar uma porta não padrão, certifique-se de incluir o número da porta.

4. Clique em **Adicionar** para adicionar mais, se necessário.
5. Depois de terminar, clique em **Concluído** para salvar e sair.

## Configurar o fuso horário

Para personalizar o formato de data e hora de acordo com suas preferências, siga estas etapas:

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Localize o bloco **Data e hora** e clique em **Editar** para configurar as seguintes opções:
   - **Formato da hora:**
     - Selecione para exibir a hora usando um relógio de 12 horas (por exemplo, 09:00 pm) ou um relógio de 24 horas (por exemplo, 21:00).
   - **Formato da data:**
     - Configure o formato da data para corresponder às suas preferências, como aaaa/MM/dd.
   - **Fuso horário:**
     - **UTC:** Exibe a data e a hora em UTC em toda a interface do usuário. Ao passar o mouse sobre a data e a hora, essas informações são exibidas no seu fuso horário local.

- **Fuso horário local:** Exibe a data e a hora no seu fuso horário local em toda a interface do usuário. Ao passar o mouse sobre a data e a hora, essas informações são exibidas em UTC.

> **Nota:**
>
> Essas configurações são específicas para cada conta de usuário.

### Habilitar resolução de DNS

Para apresentar nomes DNS em vez de endereços IP no arquivo ICA®, siga estas etapas:

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Ative a configuração **Habilitar resolução de DNS**.

### Defina o tempo limite de inatividade para o console do Studio

Você pode definir a duração da inatividade após a qual os administradores são automaticamente desconectados do console do Studio.

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Digite uma duração que varia de 10 minutos a 24 horas.
3. Para aplicar esta configuração, atualize a página ou saia e faça login novamente.

### Centralizar o gerenciamento de sites

Este recurso permite que você use um console do Web Studio para gerenciar vários sites do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Habilitar gerenciamento de vários sites.

## Tags

> **Nota:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no

> Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

## Introdução

Tags são strings que identificam itens como máquinas, aplicativos, desktops, grupos de entrega, grupos de aplicativos e políticas. Depois de criar uma tag e adicioná-la a um item, você pode adaptar certas operações para que se apliquem apenas a itens que tenham uma tag especificada.

- Personalizar exibições de pesquisa no Web Studio.

  Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma tag chamada "test" e, em seguida, adicione-a (aplique-a) a esses aplicativos. Agora você pode filtrar a pesquisa do Web Studio com a tag "test".

- Publicar aplicativos de um grupo de aplicativos ou desktops específicos de um grupo de entrega, considerando apenas um subconjunto das máquinas nos grupos de entrega selecionados. Isso é chamado de *restrição de tag*.

  Com as restrições de tag, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de mais máquinas. Uma restrição de tag pode ser considerada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Sua funcionalidade é semelhante, mas não idêntica, aos grupos de trabalho em versões do XenApp anteriores à 7.x.

  Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

- Agendar reinícios periódicos para um subconjunto de máquinas em um grupo de entrega.

  Usar uma restrição de tag para máquinas permite que você use novos cmdlets do PowerShell para configurar vários agendamentos de reinício para subconjuntos de máquinas em um grupo de entrega. Para exemplos e detalhes, consulte Gerenciar grupos de entrega.

- Personalizar a aplicação (atribuição) de políticas Citrix a um subconjunto de máquinas em grupos de entrega, tipos de grupos de entrega ou UOs que tenham (ou não tenham) uma tag especificada.

  Por exemplo, se você quiser aplicar uma política Citrix apenas às estações de trabalho mais potentes, adicione uma tag chamada "high power" a essas máquinas. Em seguida, na página **Atribuir Política** do assistente Criar Política, selecione essa tag e a caixa de seleção

**Habilitar**. Você também pode adicionar uma tag a um grupo de entrega e, em seguida, aplicar uma política Citrix a esse grupo. Para obter detalhes, consulte Criar políticas.

Você pode aplicar tags a:

- Máquinas
- Aplicativos
- Catálogos de máquinas (somente PowerShell; consulte Tags em catálogos de máquinas)
- Grupos de entrega
- Grupos de aplicativos

Uma restrição de tag pode ser configurada ao criar ou editar o seguinte no Web Studio:

- Um desktop em um grupo de entrega compartilhado
- Um grupo de aplicativos

**Importante:**

Uma tag pode ser aplicada explicitamente a uma máquina ou pode ser aplicada explicitamente no nível do catálogo de máquinas ou do grupo de entrega. Quando uma tag é aplicada no nível do catálogo de máquinas ou do grupo de entrega, todas as máquinas dentro desse catálogo ou grupo de entrega herdam implicitamente a tag. Essas tags herdadas não podem ser removidas no nível da máquina. Para remover o efeito da tag, a tag deve ser removida do nível do catálogo de máquinas ou do grupo de entrega.

## Restrições de tag para um desktop ou um grupo de aplicativos

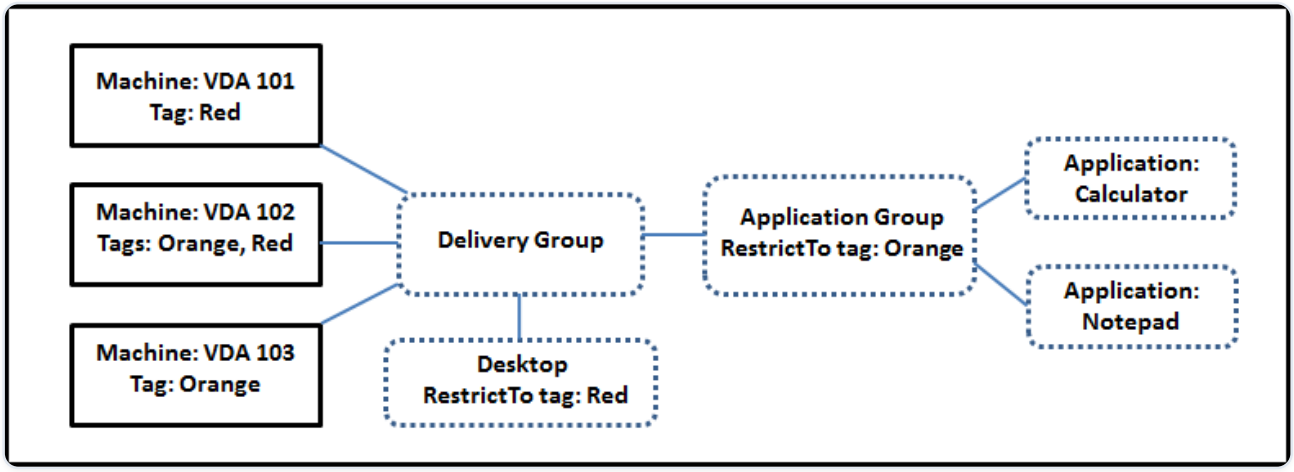
Uma restrição de tag envolve várias etapas:

- Crie a tag e, em seguida, adicione (aplique) às máquinas.
- Crie ou edite um grupo com a restrição de tag (em outras palavras, "restringir inicializações a máquinas com a tag x").

Uma restrição de tag estende o processo de seleção de máquina do broker. O broker seleciona uma máquina de um grupo de entrega associado, sujeito à política de acesso, listas de usuários configuradas, preferência de zona e prontidão de inicialização, além da restrição de tag (se presente). Para aplicativos, o broker recorre a outros grupos de entrega em ordem de prioridade, aplicando as mesmas regras de seleção de máquina para cada grupo de entrega considerado.

### Exemplo 1: Layout simples

Este exemplo apresenta um layout simples que usa restrições de tag para limitar quais máquinas são consideradas para determinadas inicializações de desktop e aplicativos. O site tem um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.



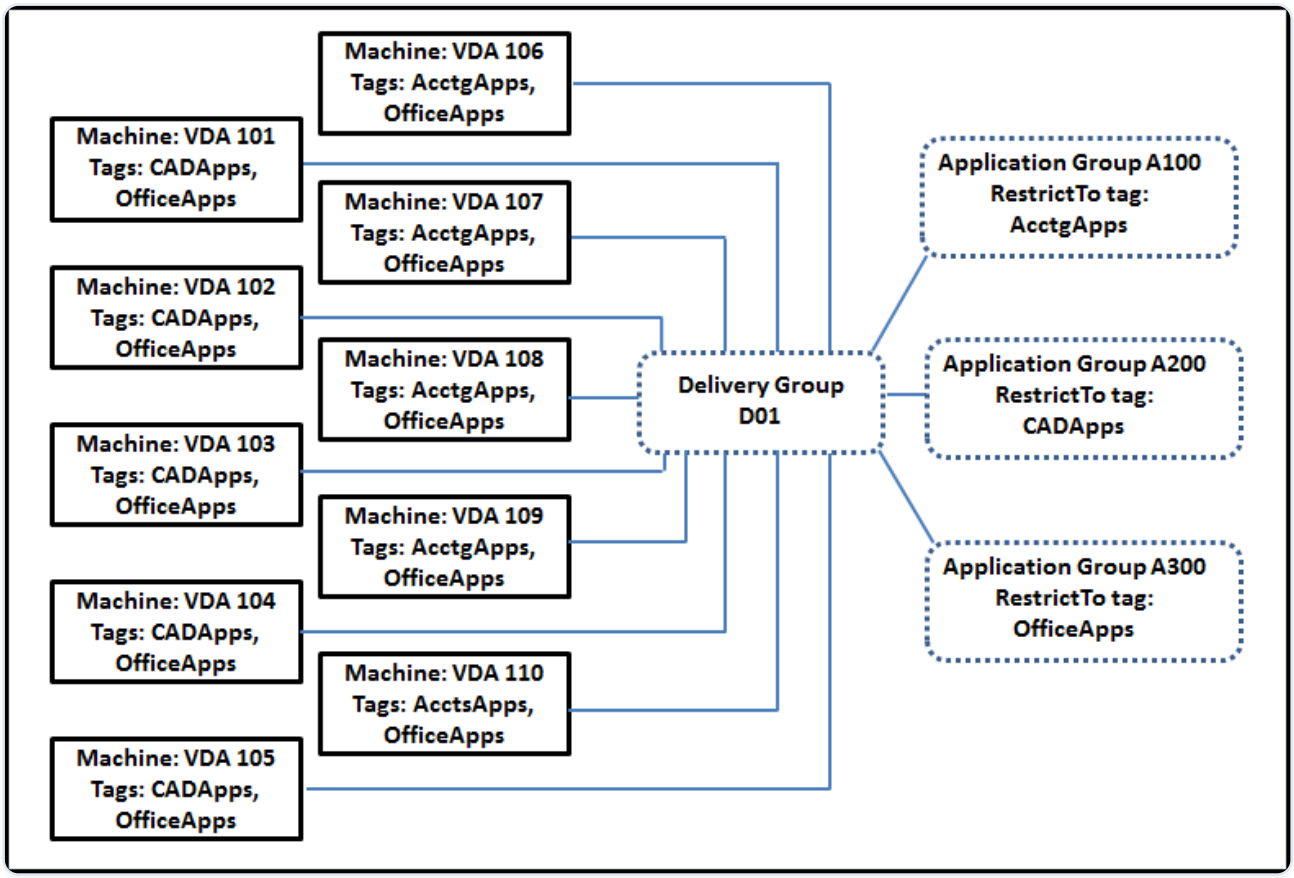

- Tags foram adicionadas a cada uma das três máquinas (VDA 101–103).
- O desktop no grupo de entrega compartilhado foi criado com uma restrição de tag chamada "Red". Um desktop pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Red": VDA 101 e 102.
- O grupo de aplicativos foi criado com a restrição de tag "Orange", então cada um de seus aplicativos (Calculadora e Bloco de Notas) pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Orange": VDA 102 e 103.

A máquina VDA 102 tem ambas as tags (Red e Orange), então ela pode ser considerada para iniciar os aplicativos e o desktop.

### Exemplo 2: Layout mais complexo

Este exemplo contém vários grupos de aplicativos que foram criados com restrições de tag. Isso resulta na capacidade de entregar mais aplicativos com menos máquinas do que seria necessário se você usasse apenas grupos de entrega.

Como configurar o exemplo 2 mostra as etapas usadas para criar e aplicar as tags e, em seguida, configurar as restrições de tag neste exemplo.




Este exemplo usa 10 máquinas (VDA 101–110), um grupo de entrega (D01) e três grupos de aplicativos (A100, A200, A300). Ao aplicar tags a cada máquina e, em seguida, especificar restrições de tag ao criar cada grupo de aplicativos:

- Os usuários de contabilidade no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 101–105)
- Os designers CAD no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 106-110)
- Os usuários do grupo que precisam de aplicativos do Office podem acessar os aplicativos do Office em 10 máquinas (VDA 101–110)

Apenas 10 máquinas são usadas, com apenas um grupo de entrega. Usar apenas grupos de entrega (sem grupos de aplicativos) exigiria o dobro de máquinas, porque uma máquina pode pertencer a apenas um grupo de entrega.

## Gerenciar tags e restrições de tags

As tags são criadas, adicionadas (aplicadas), editadas e excluídas de itens selecionados por meio da ação **Gerenciar Tags** no Web Studio.

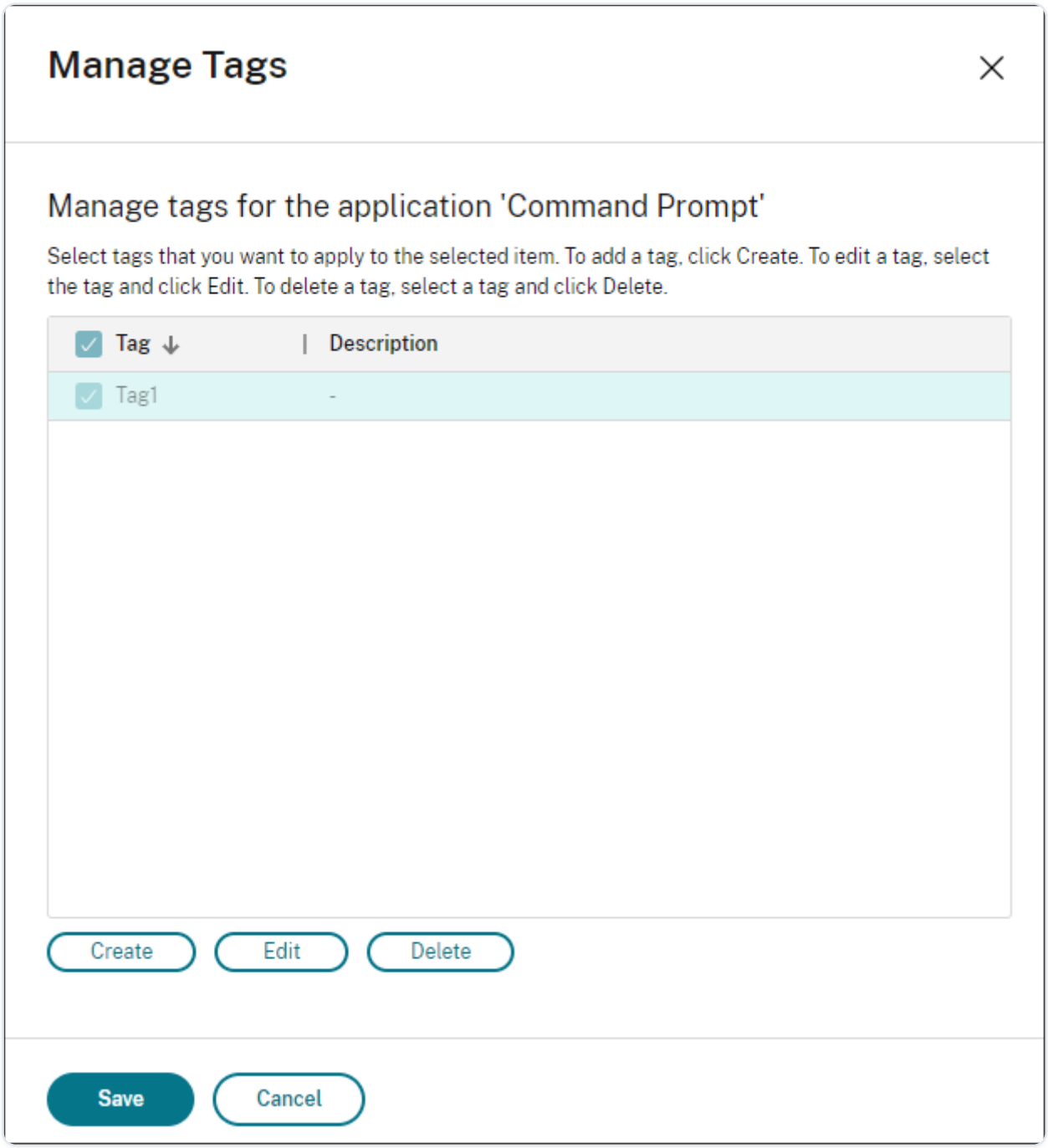
(Exceção: As tags usadas para atribuições de política são criadas, editadas e excluídas por meio da ação **Gerenciar Tags** no Web Studio. No entanto, as tags são aplicadas (atribuídas) quando você cria a política. Consulte Criar políticas para obter detalhes.)

As restrições de tag são configuradas ao criar ou editar desktops em grupos de entrega e ao criar e editar grupos de aplicativos.

### Usar as caixas de diálogo Gerenciar Tags no Web Studio

No Web Studio, selecione os itens aos quais você deseja aplicar uma tag (uma ou mais máquinas, aplicativos, um desktop, um grupo de entrega ou um grupo de aplicativos) e, em seguida, selecione **Gerenciar Tags** na barra de ações. A caixa de diálogo lista todas as tags que foram criadas no Site, não apenas para os itens selecionados.

- Uma caixa de seleção contendo uma marca de seleção indica que a tag já foi adicionada aos itens selecionados. (Na captura de tela abaixo, a máquina selecionada tem a tag chamada "Tag1" aplicada.)
- Se você selecionou mais de um item, uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados, têm essa tag adicionada.




As seguintes ações estão disponíveis na caixa de diálogo **Gerenciar Tags**. Certifique-se de revisar Precauções ao trabalhar com tags.

- **Para criar uma tag:**

  Clique em **Criar.** Insira um nome e uma descrição. Os nomes das tags devem ser exclusivos e não diferenciam maiúsculas de minúsculas. Em seguida, clique em **OK**. (A criação de uma tag não a aplica automaticamente a nenhum item selecionado. Use as caixas de seleção para aplicar a tag.)

- **Para adicionar (aplicar) uma ou mais tags:**

Marque a caixa de seleção ao lado do nome da tag. Se você selecionou vários itens e a caixa de seleção ao lado de uma tag contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a tag aplicada), alterá-la para uma marca de seleção afeta todas as máquinas selecionadas.

Se você tentar adicionar uma tag a uma ou mais máquinas, e essa tag estiver sendo usada como uma restrição em um grupo de aplicativos, você será avisado de que a ação pode resultar em tornar essas máquinas disponíveis para inicialização. Se era isso que você pretendia, prossiga.

- **Para remover uma ou mais tags:**

  Desmarque a caixa de seleção ao lado do nome da tag. Se você selecionou vários itens e a caixa de seleção ao lado de uma tag contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a tag aplicada), desmarcar a caixa de seleção remove a tag de todas as máquinas selecionadas.

  Se você tentar remover uma tag de uma máquina que está usando essa tag como uma restrição, você será avisado de que a ação pode afetar quais máquinas são consideradas para inicialização. Se era isso que você pretendia, prossiga.

- **Para editar uma tag:**

  Selecione uma tag e clique em **Editar**. Insira um novo nome, descrição ou ambos. Você pode editar apenas uma tag por vez.

- **Para excluir uma ou mais tags:**

  Selecione as tags e clique em **Excluir**. A caixa de diálogo Excluir Tag indica quantos itens usam as tags selecionadas atualmente (por exemplo, "2 máquinas"). Clique em um item para exibir mais informações. Por exemplo, clicar em um item "2 máquinas" exibe os nomes das duas máquinas que têm essa tag aplicada. Confirme se deseja excluir as tags.

  Você não pode usar o Web Studio para excluir uma tag que é usada como uma restrição. Primeiro, edite o grupo de aplicativos e remova a restrição da tag ou selecione uma tag diferente.

Quando terminar na caixa de diálogo **Gerenciar Tags**, clique em **Salvar**.

Para ver se uma máquina tem tags aplicadas: Selecione **Grupos de Entrega** no painel esquerdo. Selecione um grupo de entrega no painel central e, em seguida, selecione **Exibir Máquinas** na barra de ações. Selecione uma máquina no painel central e, em seguida, selecione a guia **Tags** no painel **Detalhes**.

## Gerenciar restrições de tag

Configurar uma restrição de tag é um processo de várias etapas: Primeiro, você cria a tag e a adiciona/aplica às máquinas. Em seguida, você adiciona a restrição ao grupo de aplicativos ou à área de trabalho.

- **Criar e aplicar a tag:**

  Crie a tag e, em seguida, adicione (aplique)-a às máquinas afetadas pela restrição de tag, usando as ações de **Gerenciar Tags** descritas anteriormente.

- **Para adicionar uma restrição de tag a um grupo de aplicativos:**

  Crie ou edite o grupo de aplicativos. Na página **Grupos de Entrega**, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista.

- **Para alterar ou remover a restrição de tag em um grupo de aplicativos:**

  Edite o grupo. Na página **Grupos de Entrega**, selecione uma tag diferente da lista ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

- **Para adicionar uma restrição de tag a um desktop:**

  Crie ou edite um grupo de entrega. Clique em **Adicionar** ou **Editar** na página **Áreas de Trabalho**. Na caixa de diálogo Adicionar Área de Trabalho, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag no menu.

- **Para alterar ou remover a restrição de tag em um grupo de entrega:**

  Edite o grupo. Na página Áreas de Trabalho, clique em **Editar**. Na caixa de diálogo, selecione uma tag diferente das listas ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

## Precauções ao trabalhar com tags

Uma tag aplicada a um item pode ser usada para diferentes propósitos, então tenha em mente que adicionar, remover e excluir uma tag pode ter efeitos não intencionais. Você pode usar uma tag para classificar as exibições de máquinas no campo de pesquisa do Web Studio. Você pode usar a mesma tag como uma restrição ao configurar um grupo de aplicativos ou uma área de trabalho. A tag limita a consideração de inicialização apenas às máquinas em grupos de entrega especificados que possuem essa tag.

Quando você tenta adicionar uma tag a máquinas depois que essa tag foi configurada como uma restrição de tag para uma área de trabalho ou um grupo de aplicativos, um aviso aparece. Adicionar essa tag pode tornar as máquinas disponíveis para iniciar aplicativos ou áreas de trabalho adicionais. Se era isso que você pretendia, prossiga. Caso contrário, você pode cancelar a operação.

Por exemplo, digamos que você crie um grupo de aplicativos com a restrição de tag "Vermelho". Mais tarde, você adiciona várias outras máquinas nos mesmos grupos de entrega usados por esse grupo de aplicativos. Se você tentar adicionar a tag "Vermelho" a essas máquinas, o Web Studio exibirá uma mensagem semelhante a: "A tag "Vermelho" é usada como uma restrição nos seguintes grupos de aplicativos. Adicionar esta tag pode tornar as máquinas selecionadas disponíveis para iniciar aplicativos neste grupo de aplicativos." Você pode então confirmar ou cancelar a adição dessa tag a essas máquinas adicionais.

Da mesma forma, se um grupo de aplicativos usa uma tag para restringir inicializações, o Web Studio avisa que você não pode excluir a tag até editar o grupo para removê-la como uma restrição. (Se você tivesse permissão para excluir uma tag que é usada como restrição em um grupo de aplicativos, isso poderia resultar em permitir que os aplicativos fossem iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição contra a exclusão de uma tag se aplica se a tag estiver sendo usada como restrição para inicializações de área de trabalho. Depois de editar o grupo de aplicativos ou as áreas de trabalho no grupo de entrega para remover essa restrição de tag, você pode excluir a tag.

Nem todas as máquinas podem ter os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada um com uma restrição de tag diferente e conjuntos de máquinas diferentes ou sobrepostos de grupos de entrega. A tabela a seguir lista como as considerações da máquina são decididas.

| QUANDO UM APLICATIVO FOI ADICIONADO A | ESSAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO |
|---|---|
| Um grupo de aplicativos sem restrição de tag | Qualquer máquina. |
| Um grupo de aplicativos com restrição de tag A | Máquinas que têm a tag A aplicada. |
| Dois grupos de aplicativos, um com restrição de tag A e o outro com restrição de tag B | Máquinas que têm a tag A e a tag B. Se nenhuma estiver disponível, então máquinas que têm a tag A ou a tag B. |

| QUANDO UM APLICATIVO FOI ADICIONADO A | ESSAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO |
|---|---|
| Dois grupos de aplicativos, um com restrição de tag A e o outro sem restrição de tag | Máquinas que têm a tag A. Se nenhuma estiver disponível, então qualquer máquina. |

Se você usou uma restrição de tag em um agendamento de reinicialização de máquina, quaisquer alterações que você fizer que afetem as aplicações ou restrições de tag afetarão o próximo ciclo de reinicialização da máquina. Isso não afeta nenhum ciclo de reinicialização que esteja em andamento enquanto as alterações estão sendo feitas.

### Como configurar o exemplo 2

A sequência a seguir mostra as etapas para criar e aplicar tags e, em seguida, configurar restrições de tag para os grupos de aplicativos ilustrados no segundo exemplo.

VDAs e aplicativos já foram instalados nas máquinas e o grupo de entrega foi criado.

Crie e aplique tags às máquinas:

1. No Web Studio, selecione o grupo de entrega D01 e, em seguida, selecione **Exibir Máquinas** na barra de ações.
2. Selecione as máquinas VDA 101–105 e, em seguida, selecione **Gerenciar Tags** na barra de ações.
3. Na caixa de diálogo Gerenciar Tags, clique em **Criar** e, em seguida, crie uma tag chamada `CADApps`. Clique em **OK**.
4. Clique em **Criar** novamente e crie uma tag chamada OfficeApps. Clique em **OK**.
5. Ainda na caixa de diálogo **Gerenciar Tags**, adicione (aplique) as tags recém-criadas às máquinas selecionadas, marcando as caixas de seleção ao lado do nome de cada tag (`CADApps` e `OfficeApps`). Quando terminar, feche a caixa de diálogo.
6. Selecione o grupo de entrega D01, selecione **Exibir Máquinas** na barra de ações.
7. Selecione as máquinas VDA 106–110 e, em seguida, selecione **Gerenciar Tags** na barra de ações.
8. Na caixa de diálogo **Gerenciar Tags**, clique em **Criar**. Crie uma tag chamada `AcctgApps`. Clique em **OK**.

9. Aplique a tag `AcctgApps` recém-criada e a tag `OfficeApps` às máquinas selecionadas, clicando nas caixas de seleção ao lado do nome de cada tag e, em seguida, feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de tag.

1. No Web Studio, selecione **Aplicativos** no painel esquerdo, selecione a guia **Grupos de Aplicativos** e, em seguida, selecione **Criar Grupo de Aplicativos** na barra de ações. O assistente Criar Grupo de Aplicativos é iniciado.
2. Na página **Grupos de Entrega** do assistente, selecione o grupo de entrega D01. Selecione **Restringir inicializações a máquinas com tag** e, em seguida, selecione a tag `AcctgApps` na lista.
3. Conclua o assistente, especificando os usuários de contabilidade e os aplicativos de contabilidade. (Ao adicionar o aplicativo, escolha a origem **Do menu Iniciar**, que pesquisa o aplicativo nas máquinas que têm a tag `AcctgApps`.) Na página **Resumo**, nomeie o grupo `A100`.
4. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando as máquinas que têm a tag `CADApps`, além dos usuários e aplicativos apropriados.
5. Repita as etapas para criar o grupo de aplicativos `A300`, especificando as máquinas que têm a tag `OfficeApps`, além dos usuários e aplicativos apropriados.

### Tags em catálogos de máquinas

Você pode usar tags em catálogos de máquinas. A sequência geral de criação de uma tag e sua aplicação a um catálogo é a mesma descrita anteriormente. No entanto, a aplicação de tags a catálogos é suportada apenas através da interface do PowerShell. Você não pode usar o Web Studio para aplicar uma tag a um catálogo ou remover uma tag de um catálogo. As exibições de catálogo no Web Studio não indicam se uma tag foi aplicada.

Resumo: Você pode usar o Web Studio ou o PowerShell para criar ou excluir uma tag para uso em um catálogo. Use o PowerShell para aplicar a tag ao catálogo.

Aqui estão alguns exemplos de uso de tags com catálogos:

- Um grupo de entrega tem máquinas de vários catálogos, mas você deseja que uma operação (como um agendamento de reinicialização) afete apenas as máquinas em um catálogo específico. A aplicação de uma tag a esse catálogo realiza isso.
- Em um grupo de aplicativos, você deseja limitar as sessões de aplicativos a máquinas em um catálogo específico. A aplicação de uma tag a esse catálogo realiza isso.

Cmdlets do PowerShell afetados:

- Você pode passar objetos de catálogo para cmdlets como `Add-BrokerTag` e `Remove-BrokerTag`.
- `Get-BrokerTagUsage` mostra quantos catálogos contêm tags.
- `Get-BrokerCatalog` tem uma propriedade chamada `Tags`.

Por exemplo, os seguintes cmdlets adicionam uma tag chamada `fy2018` ao catálogo chamado `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (A tag foi criada anteriormente usando o Web Studio ou o PowerShell.)

Consulte a ajuda do cmdlet do PowerShell para obter mais orientações e sintaxe.

## Tags automáticas (Preview)

A marcação automática permite que os administradores definam e removam tags em vários objetos do Citrix Virtual Apps and Desktops automaticamente, com base em regras personalizadas. Esse aprimoramento elimina a necessidade de manter diferentes scripts que são executados periodicamente para otimização do ambiente.

### Casos de uso

Com a marcação automática, você pode implementar regras relevantes para os seus direcionadores de negócios, como redução de custos, otimização da infraestrutura e impulsionamento do consumo. A seguir estão alguns dos casos de uso:

- **Recuperar VDIs não utilizados** - Para liberar as cargas de trabalho dedicadas que não foram usadas por mais de um número predefinido de dias para o pool disponível.
- **Remover desordem de aplicativos** - Para reduzir a desordem de aplicativos, identificando os aplicativos que não foram usados por mais de um número predefinido de dias.
- **DGs com nível funcional inferior a X** - Para encontrar grupos de entrega com um nível funcional inferior a um nível específico.
- **Usuários inativos** - Para recuperar recursos de usuários que não fizeram logon por mais de um número predefinido de dias.

### Comandos PowerShell

Você pode criar autotags usando comandos do PowerShell. Depois que uma regra de autotag é criada, ela é avaliada com uma frequência de 600 segundos. Para obter mais informações, consulte New-BrokerAutoTagRule.

### Exemplos

`New-BrokerAutoTagRule` usa o mesmo tipo de objeto e parâmetros de filtro que o cmdlet `Get-BrokerMachine`. Para obter mais informações, consulte GetBrokerMachine.

1. Marque os VDIs dedicados que não foram usados por mais de 30 dias com o ID 123:
    a. Defina uma tag para marcar os VDIs não utilizados, por exemplo, **unused-VDI**.
        - Nome da tag: unused-VDI
        - ID da tag: 123
    b. Crie a regra de auto-marcação para marcar máquinas não utilizadas. Defina os parâmetros da regra:
        - Nome : Nome genérico para a regra.
        - Tipo de objeto : Máquina.
        - Texto da regra : Máquinas estáticas, atribuídas cujo último tempo de conexão é > 30 dias ou sem valor.
        - ID da Tag : O ID da tag que você deseja associar, 123.

        ```
        New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime -eq `$null ) }” -TagUid 123
        ```
    c. Verifique as máquinas marcadas com a tag **unused-VDI** e libere-as.
2. Para marcar grupos de entrega com nível funcional inferior a X (usando **L7_20** como o nível funcional limite):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup' -RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid 123
```

1. Para marcar aplicativos visíveis ao usuário publicados sem uma pasta:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application' -RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} " -TagUid 123
```

## Mais informações

Postagem do blog: Como atribuir desktops a servidores específicos.

# Perfis de usuário

Por padrão, o Citrix Profile Management é instalado silenciosamente em imagens mestre quando você instala o Virtual Delivery Agent, mas você não precisa usar o Profile Management como uma solução de perfil.

Para atender às diversas necessidades dos seus usuários, você pode usar as políticas do Citrix Virtual Apps and Desktops™ para aplicar diferentes comportamentos de perfil às máquinas em cada Grupo de Entrega. Por exemplo, um Grupo de Entrega pode exigir perfis obrigatórios do Citrix, cujo modelo é armazenado em um local de rede, enquanto outro Grupo de Entrega exige perfis móveis do Citrix armazenados em outro local com várias pastas redirecionadas.

- Se outros administradores em sua organização são responsáveis pelas políticas do Citrix Virtual Apps and Desktops, trabalhe com eles para garantir que eles definam quaisquer políticas relacionadas a perfis em seus Grupos de Entrega.
- As políticas do Profile Management também podem ser definidas na Política de Grupo, no arquivo .ini do Profile Management e localmente em máquinas virtuais individuais. Essas múltiplas formas de definir o comportamento do perfil são lidas na seguinte ordem:

  a. Política de Grupo (arquivos .adm ou .admx)
  b. Políticas do Citrix Virtual Apps and Desktops no nó de Política
  c. Políticas locais na máquina virtual à qual o usuário se conecta
  d. Arquivo .ini do Profile Management

  Por exemplo, se você configurar a mesma política tanto na Política de Grupo quanto no nó de Política, o sistema lê a configuração da política na Política de Grupo e ignora a configuração da política do Citrix Virtual Apps and Desktops.

Qualquer que seja a solução de perfil que você escolher, os administradores do Director podem acessar informações de diagnóstico e solucionar problemas de perfis de usuário. Para obter mais informações, consulte a documentação do Director.

## Configuração automática

O tipo de desktop é detectado automaticamente, com base na instalação do Virtual Delivery Agent e, além das escolhas de configuração que você faz no Studio, define os padrões do Profile Management de acordo.

As políticas que o Profile Management ajusta são mostradas na tabela a seguir. Quaisquer configurações de política não padrão são preservadas e não são sobrescritas por este recurso.

Consulte a documentação do Profile Management para obter informações sobre cada política. Os tipos de máquinas que criam perfis afetam as políticas que são ajustadas. Os fatores primários são se as máquinas são persistentes ou provisionadas, e se são compartilhadas por vários usuários ou dedicadas a apenas um usuário.

Sistemas persistentes possuem algum tipo de armazenamento local, cujo conteúdo pode ser esperado para persistir quando o sistema é desligado. Sistemas persistentes podem empregar tecnologia de armazenamento como SANs para fornecer mimetismo de disco local. Em contraste, sistemas provisionados são criados "em tempo real" a partir de um disco base e algum tipo de disco de identidade. O armazenamento local é geralmente mimetizado por um disco RAM ou disco de rede, sendo este último frequentemente fornecido por uma SAN com um link de alta velocidade. A tecnologia de provisionamento é geralmente Citrix Provisioning ou Machine Creation Services™ (ou um equivalente de terceiros). Às vezes, sistemas provisionados possuem armazenamento local persistente. Estes são classificados como persistentes.

Juntos, esses dois fatores definem os seguintes tipos de máquina:

- **Ambos persistentes e dedicados**. Exemplos são máquinas de SO de sessão única com uma atribuição estática e armazenamento local persistente que são criadas com Machine Creation Services, estações de trabalho físicas e laptops.
- **Ambos persistentes e compartilhados**. Exemplos são máquinas de SO de múltiplas sessões que são criadas com Machine Creation Services e servidores Citrix Virtual Apps.
- **Ambos provisionados e dedicados**. Exemplos são máquinas de SO de sessão única com uma atribuição estática, mas sem armazenamento persistente, que são criadas com o Citrix Provisioning Service (no Citrix Virtual Desktops™).
- **Ambos provisionados e compartilhados**. Exemplos são máquinas de SO de sessão única com uma atribuição aleatória que são criadas com o Citrix Provisioning™ Service (no Citrix Virtual Desktops) e servidores Citrix Virtual Apps.

As seguintes configurações de política do Profile Management são diretrizes sugeridas para os diferentes tipos de máquina. Elas funcionam bem na maioria dos casos, mas você pode querer se desviar delas conforme sua implantação exigir.

> **Importante:**
>
> **Excluir perfis armazenados em cache localmente no logoff**, **Streaming de perfil** e **Sempre armazenar em cache** são impostos pelo recurso de configuração automática. Ajuste as outras políticas manualmente.

### Máquinas persistentes

| POLÍTICA | AMBOS PERSISTENTES E DEDICADOS | AMBOS PERSISTENTES E COMPARTILHADOS |
|---|---|---|
| Excluir perfis armazenados em cache localmente no logoff | Desabilitado | Ativado |
| Streaming de perfil | Desabilitado | Ativado |
| Sempre armazenar em cache | Ativado (nota 1) | Desativado (nota 2) |
| Gravação ativa | Desabilitado | Desabilitado (nota 3) |
| Processar logons de administradores locais | Ativado | Desabilitado (nota 4) |

### Máquinas provisionadas

| POLÍTICA | PROVISIONADAS E DEDICADAS | AMBOS PROVISIONADOS E COMPARTILHADOS |
|---|---|---|
| Excluir perfis armazenados em cache localmente no logoff | Desabilitado (nota 5) | Ativado |
| Streaming de perfil | Ativado | Ativado |
| Sempre armazenar em cache | Desabilitado (nota 6) | Desabilitado |
| Gravação ativa | Ativado | Ativado |
| Processar logons de administradores locais | Ativado | Habilitado (nota 7) |

1. Como o **Profile streaming** está desabilitado para este tipo de máquina, a configuração **Always cache** é sempre ignorada.
2. Desabilite **Always cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, habilitando esta política e usando-a

para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo deste tamanho ou maior é armazenado em cache localmente o mais rápido possível.

3. Desabilite **Active write back**, exceto para salvar alterações em perfis de usuários que fazem roaming entre servidores Citrix Virtual Apps. Neste caso, habilite esta política.
4. Desabilite **Process logons of local administrators**, exceto para Hosted Shared Desktops. Neste caso, habilite esta política.
5. Desabilite **Delete locally cached profiles on logoff**. Esta configuração retém os perfis armazenados em cache localmente. Como as máquinas são redefinidas no logoff, mas são atribuídas a usuários individuais, os logons são mais rápidos se seus perfis estiverem em cache.
6. Desabilite **Always cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, habilitando esta política e usando-a para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo deste tamanho ou maior é armazenado em cache localmente o mais rápido possível.
7. Habilite **Process logons of local administrators**, exceto para perfis de usuários que fazem roaming entre servidores Citrix Virtual Apps and Desktops. Neste caso, desabilite esta política.

## Redirecionamento de pastas

O redirecionamento de pastas permite armazenar dados do usuário em compartilhamentos de rede diferentes do local onde os perfis são armazenados. O redirecionamento de pastas reduz o tamanho do perfil e o tempo de carregamento, mas pode impactar a largura de banda da rede. O redirecionamento de pastas não exige que os perfis de usuário do Citrix sejam empregados. Você pode optar por gerenciar seus próprios perfis de usuário e ainda assim redirecionar pastas.

Configure o redirecionamento de pastas usando políticas Citrix no Studio.

- Certifique-se de que os locais de rede usados para armazenar o conteúdo das pastas redirecionadas estejam disponíveis e tenham as permissões corretas. As propriedades do local são validadas.
- As pastas redirecionadas são configuradas na rede e seu conteúdo é preenchido a partir dos desktops virtuais dos usuários no logon.

Configure o redirecionamento de pastas usando apenas as Políticas Citrix ou os Objetos de Política de Grupo do Active Directory, não ambos. A configuração do redirecionamento de pastas usando ambos os mecanismos de política pode resultar em comportamento imprevisível.

# Redirecionamento avançado de pastas

Em implantações com múltiplos sistemas operacionais (SOs), você pode querer que parte do perfil de um usuário seja compartilhada por cada SO. O restante do perfil não é compartilhado e é usado apenas por um SO. Para garantir uma experiência de usuário consistente entre os SOs, você precisa de uma configuração diferente para cada SO, ou seja, redirecionamento avançado de pastas. Por exemplo, diferentes versões de um aplicativo rodando em dois SOs podem precisar ler ou editar um arquivo compartilhado, então você decide redirecioná-lo para um único local de rede onde ambas as versões possam acessá-lo. Alternativamente, como o conteúdo da pasta **Start Menu** é estruturado de forma diferente em dois SOs, você decide redirecionar apenas uma pasta, não ambas. Essa abordagem separa a pasta **Start Menu** e seu conteúdo em cada SO, garantindo uma experiência consistente para os usuários.

Se sua implantação requer redirecionamento avançado de pastas, você deve entender a estrutura dos dados de perfil de seus usuários e determinar quais partes podem ser compartilhadas entre os sistemas operacionais. Comportamentos imprevisíveis podem ocorrer a menos que o redirecionamento de pastas seja usado corretamente.

Para redirecionar pastas em implantações avançadas:

- Use um Grupo de Entrega separado para cada SO.
- Entenda onde seus aplicativos virtuais, incluindo aqueles em desktops virtuais, armazenam dados e configurações do usuário, e entenda como os dados são estruturados.
- Para dados de perfil compartilhados que podem ser movidos com segurança (porque são estruturados de forma idêntica em cada SO), redirecione as pastas que os contêm em cada Grupo de Entrega.
- Para dados de perfil não compartilhados que não podem ser movidos, redirecione a pasta que os contém em apenas um dos Grupos de Desktop, geralmente aquele com o SO mais usado ou aquele onde os dados são mais relevantes. Alternativamente, para dados não compartilhados que não podem ser movidos entre SOs, redirecione as pastas que os contêm em ambos os sistemas para locais de rede separados.

## Exemplo de implantação avançada

A implantação possui aplicativos, incluindo versões do Microsoft Outlook e Internet Explorer, sendo executados em desktops Windows 10 e aplicativos, incluindo outras versões do Outlook e Internet Explorer, entregues pelo Windows Server 2019. Você já configurou dois Grupos de Entrega para os dois SOs. Os usuários desejam acessar o mesmo conjunto de **Contatos** e **Favoritos** em ambas as versões dos dois aplicativos.

**Importante:** As seguintes decisões e conselhos são válidos para os SOs e a implantação descritos. Em sua organização, as pastas que você escolher redirecionar e se você decidir compartilhá-las dependem de vários fatores que são exclusivos da sua implantação específica.

- Usando políticas aplicadas aos Grupos de Entrega, você escolhe as seguintes pastas para redirecionar.

| PASTA | REDIRECIONADO NO WINDOWS 10? | REDIRECIONADO NO WINDOWS SERVER 2019? |
|---|---|---|
| Meus Documentos | Sim | Sim |
| Dados do Aplicativo | Não | Não |
| Contatos | Sim | Sim |
| Área de Trabalho | Sim | Não |
| Downloads | Não | Não |
| Favoritos | Sim | Sim |
| Links | Sim | Não |
| Minhas Músicas | Sim | Sim |
| Minhas Imagens | Sim | Sim |
| Meus Vídeos | Sim | Sim |
| Pesquisas | Sim | Não |
| Jogos Salvos | Não | Não |
| Menu Iniciar | Sim | Não |

- Para as pastas compartilhadas e redirecionadas:
  - Após analisar a estrutura dos dados salvos pelas diferentes versões do Outlook e do Internet Explorer, você decide que é seguro compartilhar as pastas **Contatos** e **Favoritos**.
  - Você sabe que a estrutura das pastas **Meus Documentos**, **Minhas Músicas**, **Minhas Imagens** e **Meus Vídeos** é padrão em todos os sistemas operacionais. Portanto, é seguro armazenar essas pastas no mesmo local de rede para cada Grupo de Entrega.

- Para as pastas não compartilhadas e redirecionadas:
  - Você não redireciona as pastas Área de Trabalho, Links, Pesquisas ou **Menu Iniciar** no Grupo de Entrega do Windows Server porque os dados nessas pastas são organizados de forma diferente nos dois sistemas operacionais. Portanto, não podem ser compartilhados.
  - Para garantir um comportamento previsível desses dados não compartilhados, você os redireciona apenas no Grupo de Entrega do Windows 10. O Windows 10 é usado com mais frequência pelos usuários em seu trabalho diário. Os usuários acessam apenas ocasionalmente os aplicativos entregues pelo Windows Server. Além disso, neste caso, os dados não compartilhados são mais relevantes para um ambiente de desktop do que para um ambiente de aplicativo. Por exemplo, os atalhos da área de trabalho são armazenados na pasta **Área de Trabalho** e podem ser úteis se forem originados de uma máquina Windows 10, mas não de uma máquina Windows Server.
- Para as pastas não redirecionadas:
  - Você não quer sobrecarregar seus servidores com arquivos baixados pelos usuários, então você escolhe não redirecionar a pasta Downloads
  - Dados de aplicativos individuais podem causar problemas de compatibilidade e desempenho, então você decide não redirecionar a pasta Application Data

Para obter mais informações sobre o redirecionamento de pastas, consulte Visão geral de Redirecionamento de Pastas, Arquivos Offline e Perfis de Usuário Móveis.

### Redirecionamento de pastas e exclusões

No Citrix Profile Management (mas não no Studio), uma melhoria de desempenho permite evitar que as pastas sejam processadas usando exclusões. Se você usar esse recurso, não exclua nenhuma pasta redirecionada. Os recursos de redirecionamento e exclusão de pastas funcionam juntos. Garantir que nenhuma pasta redirecionada seja excluída permite que o Profile Management as mova de volta para a estrutura da pasta de perfil e preserve a integridade dos dados se você decidir não redirecioná-las posteriormente. Para obter mais informações sobre exclusões, consulte Incluir e excluir itens.

## Registro de VDA

### Introdução

> **Nota:**

> Em um ambiente local, os VDAs se registram com um Delivery Controller. Em um ambiente de serviço Citrix Cloud, os VDAs se registram com um Cloud Connector. Em um ambiente híbrido, alguns VDAs se registram com um Delivery Controller enquanto outros se registram com um Cloud Connector.

> Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) com um ou mais Controllers ou Cloud Connectors no site. O VDA encontra um Controller ou Connector verificando uma lista chamada `ListofDDCs`. O `ListOfDDCs` em um VDA contém entradas DNS que apontam esse VDA para Controllers ou Cloud Connectors no site. Para balanceamento de carga, o VDA distribui automaticamente as conexões entre todos os Controllers ou Cloud Connectors na lista.

Por que o registro do VDA é tão importante?

- De uma perspectiva de segurança, o registro é uma operação sensível. Você está estabelecendo uma conexão entre o Controller ou Cloud Connector e o VDA. Para uma operação tão sensível, o comportamento esperado é rejeitar a conexão se tudo não estiver em perfeita ordem. Você está efetivamente estabelecendo dois canais de comunicação separados: VDA para Controller ou Cloud Connector, e Controller ou Cloud Connector para VDA. A conexão usa Kerberos, então problemas de sincronização de tempo e associação de domínio são implacáveis. O Kerberos usa Nomes de Entidade de Serviço (SPNs), então você não pode usar IP\\hostname balanceado por carga.
- Se um VDA não tiver informações precisas e atuais do Controller ou Cloud Connector à medida que você adiciona e remove Controllers (ou Cloud Connectors), o VDA poderá rejeitar inicializações de sessão que são intermediadas por um Controller ou Cloud Connector não listado. Entradas inválidas podem atrasar a inicialização do software do sistema de desktop virtual. Um VDA não aceitará uma conexão de um Controller ou Cloud Connector desconhecido e não confiável.

Além do `ListofDDCs`, o `ListOfSIDs` (IDs de Segurança) indica quais máquinas no `ListofDDCs` são confiáveis. O `ListofSIDs` pode ser usado para diminuir a carga no Active Directory ou para evitar possíveis ameaças de segurança de um servidor DNS comprometido. Para mais informações, consulte ListOfSIDs.

Se um `ListofDDCs` especificar mais de um Controller ou Cloud Connector, o VDA tenta se conectar a eles em ordem aleatória. Em uma implantação local, o `ListofDDCs` também pode

conter grupos de Controller. O VDA tenta se conectar a cada Controller em um grupo antes de passar para outras entradas no `ListofDDCs`.

O Citrix Virtual Apps and Desktops™ testa automaticamente a conectividade com os Controllers ou Cloud Connectors configurados durante a instalação do VDA. Erros são exibidos se um Controller ou Cloud Connector não puder ser alcançado. Se você ignorar um aviso de que um Controller ou Cloud Connector não pode ser contatado (ou quando você não especifica endereços de Controller ou Cloud Connector durante a instalação do VDA), mensagens o lembrarão.

## Métodos para configurar endereços de Controller ou Cloud Connector

O administrador escolhe o método de configuração a ser usado quando o VDA se registra pela primeira vez (o registro inicial). Durante o registro inicial, um cache persistente é criado no VDA. Durante os registros subsequentes, o VDA recupera a lista de Controllers ou Cloud Connectors deste cache local, a menos que uma alteração de configuração seja detectada.

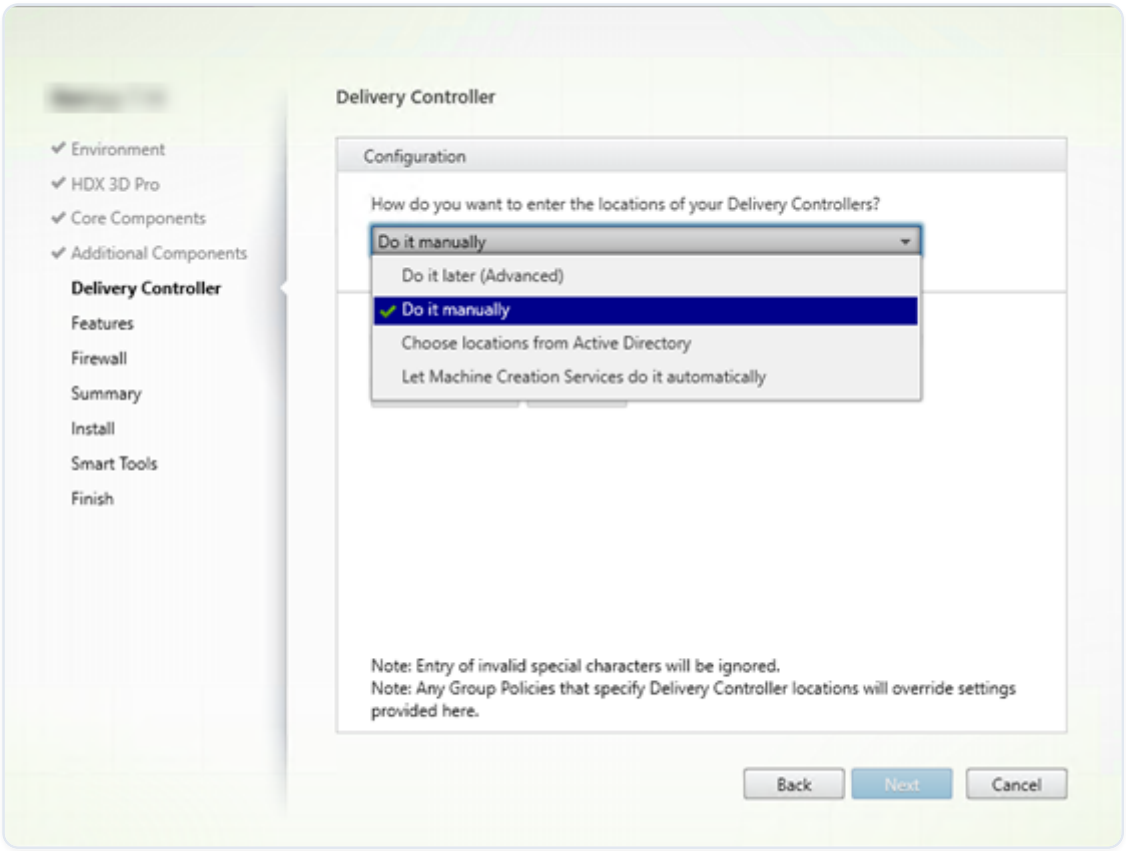
A maneira mais fácil de recuperar essa lista durante os registros subsequentes é usando o recurso de atualização automática. A atualização automática é habilitada por padrão. Para mais informações, consulte Atualização automática.

Existem vários métodos para configurar endereços de Controller ou Cloud Connector em um VDA.

- Baseado em política (LGPO ou GPO)
- Baseado em registro (manual, Preferências de Política de Grupo (GPP), especificado durante a instalação do VDA)
- Baseado em OU do Active Directory (descoberta de OU legada)
- Baseado em MCS (personality.ini)

Você especifica o método de registro inicial ao instalar um VDA. (Se você desabilitar a atualização automática, o método selecionado durante a instalação do VDA será usado para registros subsequentes.)

O gráfico a seguir mostra a página **Delivery Controller** do assistente de instalação do VDA.




### Baseado em política (LGPO\GPO)

A Citrix® recomenda usar GPO para o registro inicial do VDA. Ele tem a prioridade mais alta. (Embora a atualização automática seja listada como a prioridade mais alta, a atualização automática é usada somente após o registro inicial.) O registro baseado em política oferece as vantagens de centralização do uso da Política de Grupo para configuração.

Para especificar este método, conclua as duas etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer mais tarde (avançado)**. O assistente o lembrará várias vezes de especificar os endereços do Controller, mesmo que você não os esteja especificando durante a instalação do VDA. (O registro do VDA é muito importante.)
- Habilite ou desabilite o registro de VDA baseado em política por meio da política Citrix com a configuração `Virtual Delivery Agent Settings > Controllers`. (Se a segurança for sua principal prioridade, use a configuração `Virtual Delivery Agent Settings > Controller SIDs`.)

Essa configuração é armazenada em `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

### Baseado em registro

Para especificar este método, conclua uma das etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer manualmente**. Em seguida, insira o FQDN de um Controller instalado e clique em **Adicionar**. Se você instalou mais Controllers, adicione os endereços deles.
- Para uma instalação de VDA por linha de comando, use a opção /controllers e especifique os FQDNs dos Controllers ou Cloud Connectors instalados.

Esta informação é armazenada no valor de registro `ListOfDDCs` sob a chave de registro `HKLM\Software\Citrix\VirtualDesktopAgent` ou `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

Você também pode configurar esta chave de registro manualmente ou usar as Preferências de Política de Grupo (GPP). Este método pode ser preferível ao método baseado em política (por exemplo, se você quiser processamento condicional de diferentes Controladores ou Cloud Connectors, como: usar XDC-001 para nomes de computador que começam com XDW-001-).

Atualize a chave de registro `ListOfDDCs`, que lista os FQDNs de todos os Controladores ou Cloud Connectors no site. (Esta chave é o equivalente à OU do site do Active Directory.)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

Se o local de registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` contiver as chaves `ListOfDDCs` e `FarmGUID`, `ListOfDDCs` será usado para a descoberta de Controladores ou Cloud Connectors. `FarmGUID` estará presente se uma OU de site foi especificada durante a instalação do VDA. (Isso pode ser usado em implantações legadas.)

Opcionalmente, atualize a chave de registro `ListOfSIDs` (para mais informações, consulte ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

Lembre-se: Se você também habilitar o registro de VDA baseado em política através da política Citrix, isso substituirá as configurações que você especificar durante a instalação do VDA, porque é um método de prioridade mais alta.

### Baseado em OU do Active Directory (legado)

Este método é suportado principalmente para compatibilidade com versões anteriores e não é recomendado. Se você ainda o estiver usando, a Citrix sugere mudar para outro método.

Para especificar este método, conclua as duas etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Escolher locais do Active Directory.**
- Use o script `Set-ADControllerDiscovery.ps1` (disponível em cada Controller). Além disso, configure a entrada de registro `FarmGuid` em cada VDA para apontar para a OU correta. Esta configuração pode ser feita usando a Política de Grupo.

### Baseado em MCS

Se você usa o MCS para provisionar VMs, o MCS configura a lista de Controladores ou Cloud Connectors. Este recurso funciona com a atualização automática. Ao criar o catálogo, o MCS injeta a lista de Controladores ou Cloud Connectors no arquivo `Personality.ini` durante o provisionamento inicial. A atualização automática mantém a lista atualizada.

Para especificar esse método, na página **Delivery Controller** do assistente de instalação do VDA, selecione **Deixar o Machine Creation Services™ fazer isso**.

### Revisão e recomendações

Como melhor prática:

- Use o método de registro de Política de Grupo para o registro inicial.
- Use a atualização automática (habilitada por padrão) para manter sua lista de Controladores atualizada.
- Em uma implantação multizona, use a Política de Grupo para a configuração inicial (com pelo menos dois Controladores ou Cloud Connectors). Aponte os VDAs para Controladores ou Cloud Connectors locais (na) sua zona. Use a atualização automática para mantê-los atualizados. A atualização automática otimiza automaticamente o `ListofDDCs` para VDAs em zonas satélite.
- Liste mais de um controlador na chave de registro `ListOfDDCs`, separados por um espaço ou uma vírgula, para evitar problemas de registro se um Controlador não estiver disponível. Por exemplo:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs
```

```
HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- Certifique-se de que todos os valores listados em `ListofDDCs` mapeiem para um nome de domínio totalmente qualificado válido para evitar atrasos no registro de inicialização.

## Atualização automática

A atualização automática (introduzida no XenApp e XenDesktop 7.6) é habilitada por padrão. É o método mais eficiente para manter seus registros de VDA atualizados. Embora não seja usado para o registro inicial, o software de atualização automática baixa e armazena o `ListofDDCs` em um cache persistente no VDA quando o registro inicial ocorre. Esse processo é feito para cada VDA. O cache também contém informações de política da máquina, o que garante que as configurações de política sejam mantidas após as reinicializações.

A atualização automática é suportada ao usar MCS ou Citrix Provisioning™ para provisionar máquinas, exceto para o cache do lado do servidor do Citrix Provisioning. O cache do lado do servidor não é um cenário comum porque não há armazenamento persistente para o cache de atualização automática.

Para especificar esse método:

- Habilite ou desabilite a atualização automática por meio de uma política Citrix que contenha a configuração `Virtual Delivery Agent Settings > Enable auto update of Controllers`. Essa configuração é habilitada por padrão.

Como funciona:

- Cada vez que um VDA se registra novamente (por exemplo, após a reinicialização de uma máquina), o cache é atualizado. Cada Controlador ou Cloud Connector também verifica o banco de dados do site a cada 90 minutos. Se um Controlador ou Cloud Connector foi adicionado ou removido desde a última verificação, ou se ocorreu uma alteração de política que afeta o registro do VDA, o Controlador ou Cloud Connector envia uma lista atualizada para seus VDAs registrados e o cache é atualizado. O VDA aceita conexões de todos os Controladores ou Cloud Connectors em sua lista mais recentemente armazenada em cache.
- Se um VDA receber uma lista que não inclui o Controlador ou Cloud Connector ao qual está registrado (em outras palavras, esse Controlador ou Cloud Connector foi removido do site), o

VDA se registrará novamente, escolhendo entre os Controladores ou Cloud Connectors no `ListofDDCs`.

Exemplo:

- Uma implantação tem três Controladores: A, B e C. Um VDA se registra com o Controlador B (que foi especificado durante a instalação do VDA).
- Posteriormente, dois Controladores (D e E) são adicionados ao site. Em 90 minutos, os VDAs recebem listas atualizadas e, em seguida, aceitam conexões dos Controladores A, B, C, D e E. (A carga não é distribuída igualmente para todos os Controladores até que os VDAs sejam reiniciados.)
- Mais tarde ainda, o Controller B é movido para outro site. Em 90 minutos, os VDAs no site original recebem listas atualizadas porque houve uma alteração de Controller desde a última verificação. O VDA que se registrou originalmente com o Controller B (que não está mais na lista) se registra novamente, escolhendo entre os Controllers na lista atual (A, C, D e E).

Em uma implantação multizona, a atualização automática em uma zona satélite armazena em cache automaticamente todos os Controllers locais primeiro. Todos os Controllers na zona primária são armazenados em cache em um grupo de backup. Se nenhum Controller local na zona satélite estiver disponível, o registro é tentado com os Controllers na zona primária.

Conforme mostrado no exemplo a seguir, o arquivo de cache contém nomes de host e uma lista de IDs de segurança (`ListofSIDs`). O VDA não consulta SIDs, o que reduz a carga do Active Directory.

```
<?xml version="1.0"?>
<ListOfDDCsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      - <d2p1:ArrayOfstring>
            <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
            <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
        </d2p1:ArrayOfstring>
    </_x003C_GroupsOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
    </_x003C_ListOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
        <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
        <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
    </_x003C_ListOfSids_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDCsListIfSids>
```

Você pode recuperar o arquivo de cache com uma chamada WMI. No entanto, ele é armazenado em um local que é legível apenas pela conta SYSTEM.

> **Importante:**

> Esta informação é fornecida apenas para fins informativos. NÃO MODIFIQUE ESTE ARQUIVO. Quaisquer modificações neste arquivo ou pasta resultam em uma configuração não suportada.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

Se você precisar configurar manualmente o `ListofSIDs` por motivos de segurança (distinto da redução da carga do Active Directory), você não poderá usar o recurso de atualização automática. Para obter detalhes, consulte ListOfSIDs.

### Exceção à prioridade de atualização automática

Embora a atualização automática geralmente tenha a maior prioridade de todos os métodos de registro de VDA e substitua as configurações para outros métodos, há uma exceção. Os elementos `NonAutoListOfDDCs` no cache especificam o método de configuração inicial do VDA. A atualização automática monitora essas informações. Se o método de registro inicial mudar, o processo de registro ignora a atualização automática e usa o próximo método de prioridade configurado mais alto. Esse processo pode ser útil ao mover um VDA para outro site (por exemplo, durante a recuperação de desastres).

## Considerações de configuração

Visualize uma configuração comum de registro de VDA.

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Visualize as etapas de registro do VDA.

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Considere o seguinte ao configurar itens que podem afetar o registro do VDA.

### Endereços de Controller ou Cloud Connector

Independentemente do método que você usa para especificar Controllers ou Cloud Connectors, a Citrix recomenda usar um endereço FQDN. Um endereço IP não é considerado uma configuração confiável, pois é mais fácil comprometer um IP do que um registro DNS. Se você preencher o `ListofSIDs` manualmente, poderá usar um IP em um `ListofDDCs`. No entanto, o FQDN ainda é recomendado.

### Balanceamento de carga

Conforme observado anteriormente, o VDA distribui automaticamente as conexões entre todos os Controllers ou Cloud Connectors no `ListofDDCs`. A funcionalidade de failover e balanceamento de carga é incorporada ao Citrix Brokering Protocol (CBP). Se você especificar vários Controllers ou Cloud Connectors em sua configuração, o registro fará o failover automaticamente entre eles, se necessário. Com a atualização automática, o failover automático ocorre automaticamente para todos os VDAs.

Por motivos de segurança, você não pode usar um balanceador de carga de rede, como o Citrix ADC. O registro do VDA usa autenticação mútua Kerberos, onde o cliente (VDA) deve provar sua identidade ao serviço (Controller). No entanto, o Controller ou Cloud Connector deve provar sua identidade ao VDA. Isso significa que o VDA e o Controller ou Cloud Connector estão agindo como servidor e cliente ao mesmo tempo. Conforme observado no início deste artigo, existem dois canais de comunicação: VDA para Controller/Cloud Connector e Controller/Cloud Connector para VDA.

Um componente neste processo é chamado Service Principal Name (SPN), que é armazenado como uma propriedade em um objeto de computador do Active Directory. Quando seu VDA se conecta a um Controller ou Cloud Connector, ele deve especificar com quem deseja se comunicar. Este endereço é um SPN. Se você usar um IP balanceado por carga, a autenticação mútua Kerberos reconhece corretamente que o IP não pertence ao Controller ou Cloud Connector esperado.

Para obter mais informações, consulte:

- Introdução ao Kerberos
- Autenticação mútua usando Kerberos

### A atualização automática substitui o CNAME

O recurso de atualização automática substitui a função CNAME (alias DNS) das versões do XenApp e XenDesktop anteriores à 7.x. A funcionalidade CNAME está desabilitada, a partir do XenApp e XenDesktop 7. Use a atualização automática em vez de CNAME. (Se você precisar usar CNAME, consulte CTX137960. Para que o aliasing de DNS funcione de forma consistente, não use atualização automática e CNAME ao mesmo tempo.)

### Grupos de Controller/Cloud Connector

Em certos cenários, você pode querer processar Controllers ou Cloud Connectors em grupos, com um grupo sendo preferencial e o outro grupo usado para failover se todos os Controllers/Cloud

Connectors falharem. Lembre-se de que os Controllers ou Cloud Connectors são selecionados aleatoriamente da lista, então o agrupamento pode ajudar a impor o uso preferencial.

Esses grupos são destinados ao uso dentro de um único site (não em vários sites).

Use parênteses para especificar grupos de Controllers/Cloud Connectors. Por exemplo, com quatro Controllers (dois primários e dois de backup), um agrupamento pode ser:

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

Neste exemplo, os Controllers do primeiro grupo (001 e 002) são processados primeiro. Se ambos falharem, os Controllers do segundo grupo (003 e 004) são processados.

Para XenDesktop 7.0 ou superior, há uma etapa extra que você precisa executar para usar o recurso **Grupos de Registro**. Você precisa **Proibir** a política **Habilitar Atualização Automática do Controller** no Studio.

## ListOfSIDs

A lista de Controllers que um VDA pode contatar para registro é o `ListofDDCs`. Um VDA também deve saber em quais Controllers confiar; os VDAs não confiam automaticamente nos Controllers em `ListofDDCs`. Os `ListofSIDs` (IDs de Segurança) identificam os Controllers confiáveis. Os VDAs tentam se registrar apenas com Controllers confiáveis.

Na maioria dos ambientes, o `ListofSIDs` é gerado automaticamente a partir do `ListofDDCs`. Você pode usar um rastreamento CDF para ler o `ListofSIDs`.

Geralmente, não há necessidade de modificar manualmente o `ListofSIDs`. Existem várias exceções. As duas primeiras exceções não são mais válidas porque tecnologias mais recentes estão disponíveis.

- **Funções separadas para Controllers:** Antes da introdução das zonas no XenApp e XenDesktop 7.7, o `ListofSIDs` era configurado manualmente quando apenas um subconjunto de Controllers era usado para registro. Por exemplo, se você estivesse usando XDC-001 e XDC-002 como brokers XML, e XDC-003 e XDC-004 para registro de VDA, você especificava todos os Controllers em `ListofSIDs`, e XDC-003 e XDC-004 em `ListofDDCs`. Esta não é uma configuração típica ou recomendada. Não a use em ambientes mais recentes. Em vez disso, use zonas.
- **Reduzindo a carga do Active Directory:** Antes da introdução do recurso de atualização automática no XenApp e XenDesktop 7.6, o `ListofSIDs` era usado para reduzir a carga nos controladores de domínio. Ao pré-popular o `ListofSIDs`, a resolução de nomes DNS para

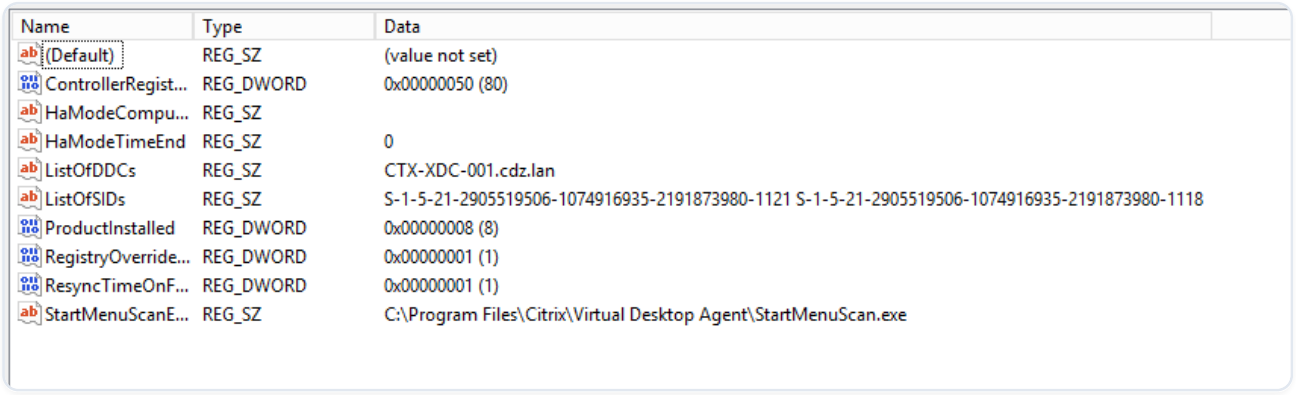
SIDs pode ser ignorada. No entanto, o recurso de atualização automática elimina a necessidade desse trabalho, pois esse cache persistente contém SIDs. A Citrix recomenda manter o recurso de atualização automática ativado.

- **Segurança:** Em alguns ambientes altamente seguros, os SIDs dos Controllers confiáveis eram configurados manualmente para evitar possíveis ameaças de segurança de um servidor DNS comprometido. No entanto, se você fizer isso, também deverá desativar o recurso de atualização automática. Caso contrário, a configuração do cache persistente será usada.

Portanto, a menos que você tenha um motivo específico, não modifique o `ListofSIDs`.

Se você precisar modificar o `ListofSIDs`, crie uma chave de registro chamada `ListOfSIDs (REG_SZ)` em `HKLM\Software\Citrix\VirtualDesktopAgent`. O valor é uma lista de SIDs confiáveis, separados por espaços se houver mais de um.

No exemplo a seguir, um Controlador é usado para registro de VDA (`ListofDDCs`), mas dois Controladores são usados para intermediação (List OfSIDs).



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| ControllerRegist... | REG_DWORD | 0x00000050 (80) |
| HaModeCompu... | REG_SZ | |
| HaModeTimeEnd | REG_SZ | 0 |
| ListOfDDCs | REG_SZ | CTX-XDC-001.cdz.lan |
| ListOfSIDs | REG_SZ | S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118 |
| ProductInstalled | REG_DWORD | 0x00000008 (8) |
| RegistryOverride... | REG_DWORD | 0x00000001 (1) |
| ResyncTimeOnF... | REG_DWORD | 0x00000001 (1) |
| StartMenuScanE... | REG_SZ | C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe |

## Pesquisa de Controlador durante o registro de VDA

Quando um VDA tenta se registrar, o Broker Agent primeiro executa uma pesquisa DNS no domínio local para garantir que o Controlador especificado possa ser alcançado.

Se essa pesquisa inicial não encontrar o Controller, o Broker Agent pode iniciar uma consulta de fallback de cima para baixo no AD. Essa consulta pesquisa todos os domínios e se repete frequentemente. Se o endereço do Controller for inválido (por exemplo, o administrador inseriu um FQDN incorreto ao instalar o VDA), a atividade dessa consulta pode potencialmente levar a uma condição de negação de serviço distribuída (DDoS) no controlador de domínio.

A seguinte chave de registro controla se o Broker Agent usa a consulta de fallback de cima para baixo quando não consegue localizar um Controlador durante a pesquisa inicial.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- Nome: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valor: `0` (padrão) ou qualquer valor diferente de zero

Quando definido como `0`, a pesquisa de fallback é ativada. Se a pesquisa inicial pelo Controller falhar, a pesquisa de fallback de cima para baixo é iniciada. Este é o comportamento padrão. No entanto, se definido para qualquer valor diferente de zero, a pesquisa de fallback é desativada. Se a pesquisa inicial pelo Controller falhar, o Broker Agent para de procurar.

## Sequenciamento de vinculação LDAP durante o registro de VDA usando um controlador de domínio somente leitura

Quando um VDA se registra com um controlador de domínio somente leitura (RODC), o Broker Agent deve selecionar qual vinculação ou vinculações do Light Directory Access Protocol (LDAP) ignorar. Para fazer essa seleção, o Broker Agent requer uma chave de registro adequada.

Se uma chave de registro não for fornecida, ou o campo da chave de registro estiver vazio, o registro do VDA com o RODC leva mais tempo porque é necessário passar pela sequência de vinculação LDAP original.

Para modificar a sequência de vinculação LDAP, a chave de registro `ListofIgnoredBindings` foi adicionada a `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. O uso de `ListofIgnoredBindings` permite modificar a sequência de vinculação LDAP conforme necessário e, assim, acelerar o registro do VDA com um RODC.

- Nome: `ListofIgnoredBindings`
- Tipo: `REG_SZ`
- Valores: `DefaultPath`, `DomainPath`, `PDCPath`

O valor é uma lista de opções de caminho de vinculação, cada uma separada por uma vírgula. A chave de registro ignorará quaisquer valores que não reconheça como válidos.

## Solucionar problemas de registro de VDA

Conforme observado anteriormente, um VDA deve ser registrado em um Delivery Controller ou Cloud Connector para ser considerado ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos que de outra forma estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador

pode solucionar. O Studio fornece informações de solução de problemas no assistente de criação de catálogo e depois que você cria um Delivery Group.

- **Identificando problemas durante a criação do catálogo de máquinas:** No assistente de criação de catálogo, depois de adicionar máquinas existentes, a lista de nomes de contas de computador indica se cada máquina é adequada para ser adicionada ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre essa máquina.

  Se a mensagem identificar uma máquina problemática, você pode remover essa máquina (usando o botão **Remover**) ou adicionar a máquina. Por exemplo, se uma mensagem indicar que as informações sobre uma máquina não foram obtidas (talvez porque ela nunca tenha sido registrada), você pode optar por adicionar a máquina de qualquer forma.

  O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto pode exigir um novo VDA. Definir um nível funcional torna todos os recursos introduzidos nessa versão (e posteriores, se o nível funcional não mudar) disponíveis para as máquinas no catálogo. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não poderão se registrar.
- **Identificando problemas após a criação de Grupos de Entrega:** Depois de criar um Grupo de Entrega, o Studio exibe detalhes sobre as máquinas associadas a esse grupo.

  O painel de detalhes de um Grupo de Entrega indica o número de máquinas que deveriam estar registradas, mas não estão. Em outras palavras, pode haver uma ou mais máquinas ligadas e não em modo de manutenção, mas que não estão atualmente registradas em um Controller. Ao visualizar uma "não registrada, mas deveria estar", revise a guia **Solucionar problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

### Mais informações sobre a solução de problemas de registro de VDA

- Para obter mais informações sobre níveis funcionais, consulte Versões de VDA e níveis funcionais.
- Para obter mais informações sobre a solução de problemas de registro de VDA, consulte CTX136668.
- Você também pode usar as verificações de integridade do Citrix Scout para solucionar problemas de registro de VDA e inicialização de sessão. Para obter detalhes, consulte Sobre as verificações de integridade.

# IP virtual e loopback virtual

**Importante:**

- O Windows 10 Enterprise multi-session não oferece suporte à Virtualização de IP da Área de Trabalho Remota (IP Virtual) e não oferecemos suporte à Virtualização de IP da Área de Trabalho Remota ou loopback virtual no Windows 10 Enterprise multi-session.
- A Virtualização de IP da Área de Trabalho Remota (IP Virtual) não é compatível com máquinas hospedadas na nuvem. Para obter mais informações, consulte a documentação da Microsoft.

Os recursos de Virtualização de IP da Área de Trabalho Remota e loopback virtual são compatíveis com máquinas Windows Server 2016, Windows Server 2019 e Windows Server 2022. Esses recursos não se aplicam a máquinas com sistema operacional Windows para desktop.

O recurso de endereço de Virtualização de IP da Área de Trabalho Remota da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. Com o recurso de loopback virtual da Citrix, você pode configurar aplicativos que dependem de comunicações com localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo de localhost (127.*).

Certos aplicativos, como CRM e Integração de Telefonia Computacional (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros propósitos que exigem um endereço IP ou endereço de loopback exclusivo. Outros aplicativos podem se vincular a uma porta estática, de modo que as tentativas de iniciar instâncias adicionais de um aplicativo em um ambiente multiusuário falham porque a porta está em uso. Para que esses aplicativos funcionem corretamente em um ambiente Citrix Virtual Apps™, é necessário um endereço IP exclusivo para cada dispositivo.

A Virtualização de IP de Área de Trabalho Remota e o loopback virtual são recursos independentes um do outro. Você pode usar um ou ambos.

Sinopse da ação do administrador:

- Para usar a Virtualização de IP da Área de Trabalho Remota da Microsoft, habilite e configure-a no servidor Windows. (As configurações de política do Citrix® não são necessárias.)

- Para usar o loopback virtual da Citrix, configure duas configurações em uma política da Citrix.

## Virtualização de IP de Área de Trabalho Remota (IP Virtual)

Quando a Virtualização de IP de Área de Trabalho Remota é habilitada e configurada no servidor Windows, cada aplicativo configurado em execução em uma sessão parece ter um endereço exclusivo. Os usuários acessam esses aplicativos em um servidor Citrix Virtual Apps da mesma forma que acessam qualquer outro aplicativo publicado. Um processo requer Virtualização de IP de Área de Trabalho Remota em qualquer um dos seguintes casos:

- O processo usa um número de porta TCP codificado
- O processo usa sockets do Windows e requer um endereço IP exclusivo ou um número de porta TCP especificado

Para determinar se um aplicativo precisa usar endereços de Virtualização de IP de Área de Trabalho Remota:

1. Obtenha a ferramenta **TCPView** da Microsoft. Esta ferramenta lista todos os aplicativos que vinculam endereços IP e portas específicos. Para obter mais informações sobre o TCPView, consulte a documentação da Microsoft.
2. Desative o recurso **Resolver Endereços IP** para que você veja os endereços em vez dos nomes de host.
3. Inicie o aplicativo e use o **TCPView** para ver quais endereços IP e portas o aplicativo abre e quais nomes de processo estão abrindo essas portas.
4. Configure quaisquer processos que abram o endereço IP do servidor, 0.0.0.0 ou 127.0.0.1.
5. Para garantir que um aplicativo não abra o mesmo endereço IP em uma porta diferente, inicie outra instância do aplicativo.

### Como funciona a virtualização de IP do Microsoft Remote Desktop (RD)

- O endereçamento IP virtual deve ser habilitado no servidor Microsoft.

  Por exemplo, em um ambiente Windows Server 2016, no Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões do Host da Sessão RD** para habilitar o recurso de Virtualização de IP RD e configure as definições para atribuir dinamicamente endereços IP usando o servidor Dynamic Host Configuration Protocol (DHCP) por sessão ou por programa. Para obter mais informações sobre como configurar a Virtualização de IP da Área de Trabalho Remota, consulte a documentação da Microsoft.

- Após habilitar o recurso, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente do servidor DHCP.
- O recurso **Virtualização de IP RD** atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilharão um endereço IP por sessão.
- Depois que um endereço é atribuído a uma sessão, a sessão usa o endereço virtual em vez do endereço IP principal do sistema sempre que as seguintes chamadas são feitas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Ao usar o recurso de virtualização de IP da Microsoft na configuração de hospedagem de sessão da Área de Trabalho Remota, os aplicativos são vinculados a endereços IP específicos inserindo um componente de “filtro” entre o aplicativo e as chamadas de função Winsock. O aplicativo então vê apenas o endereço IP correto a ser usado. Qualquer tentativa do aplicativo de escutar comunicações TCP ou UDP é automaticamente vinculada ao seu endereço IP virtual alocado (ou endereço de loopback). Quaisquer conexões de origem abertas pelo aplicativo se originam do endereço IP vinculado ao aplicativo.

Em funções que retornam um endereço (como `GetAddrInfo()`, que uma política do Windows controla), se o endereço IP do host local for solicitado, a Virtualização de IP da Área de Trabalho Remota examina o endereço IP retornado e o altera para o endereço de Virtualização de IP da Área de Trabalho Remota da sessão. Aplicativos que tentam obter o endereço IP do servidor local por meio de tais funções de nome veem apenas o endereço de Virtualização de IP da Área de Trabalho Remota exclusivo atribuído a essa sessão. Este endereço IP é frequentemente usado em chamadas de soquete subsequentes, como bind ou connect. Para obter mais informações sobre as políticas do Windows, consulte Virtualização de IP RDS no Windows Server.

Frequentemente, um aplicativo solicita vincular-se a uma porta para escuta no endereço 0.0.0.0. Quando um aplicativo faz isso e usa uma porta estática, você não pode iniciar mais de uma instância do aplicativo. O recurso de endereço de Virtualização de IP da Área de Trabalho Remota também procura por 0.0.0.0 nesses tipos de chamada. Ele altera a chamada para escutar no endereço de Virtualização de IP da Área de Trabalho Remota específico, o que permite que mais de um aplicativo escute na mesma porta no mesmo computador, pois todos estão escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço de Virtualização de IP da Área de Trabalho Remota estiver habilitado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentarem vincular-se a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas serão vinculadas a VIPAddress1:9000 e VIPAddress2:9000 e não haverá conflito.

# Loopback virtual

A ativação das configurações da **política de loopback de virtualização de IP do Citrix Remote Desktop** permite que cada sessão tenha seu próprio endereço de loopback para comunicação. Quando um aplicativo usa o endereço localhost (padrão = 127.0.0.1) em uma chamada Winsock, o recurso de loopback virtual simplesmente substitui 127.0.0.1 por 127.X.X.X, onde X.X.X é uma representação do ID da sessão + 1. Por exemplo, um ID de sessão de 7 é 127.0.0.8. No caso improvável de o ID da sessão exceder o quarto octeto (mais de 255), o endereço passa para o próximo octeto (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em qualquer um dos seguintes casos:

- O processo usa o endereço de loopback de soquete do Windows (localhost) (127.0.0.1)
- O processo usa um número de porta TCP codificado

Use as configurações da política de loopback virtual para aplicativos que usam um endereço de loopback para comunicação entre processos. Nenhuma configuração adicional é necessária. O loopback virtual não tem dependência de IP Virtual, então você não precisa configurar o servidor Microsoft.

- Suporte a loopback de IP virtual. Quando ativada, esta configuração de política permite que cada sessão tenha seu próprio endereço de loopback virtual. Esta configuração está desativada por padrão. O recurso se aplica apenas a aplicativos especificados com a configuração de política da lista de programas de loopback virtual de IP virtual.
- Lista de programas de loopback virtual de IP virtual. Esta configuração de política especifica os aplicativos que usam o recurso de loopback de IP virtual. Esta configuração se aplica apenas quando a configuração de política de suporte a loopback de IP virtual está ativada.

### Recurso relacionado

Você pode usar as seguintes configurações de registro para garantir que o loopback virtual tenha preferência sobre o IP virtual. Esse recurso é chamado de loopback preferencial. No entanto, prossiga com cautela:

- Use o loopback preferencial somente se o IP virtual e o loopback virtual estiverem habilitados. Caso contrário, você poderá ter resultados inesperados.
- A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Execute regedit nos servidores onde os aplicativos residem.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- Nome: PreferLoopback, Tipo: REG_DWORD, Dados: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dados: \<lista de processos\>

# Zonas

> **Observação:**

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

> Implantações que abrangem locais amplamente dispersos conectados por uma WAN podem enfrentar desafios devido à latência e confiabilidade da rede. Existem duas opções que mitigam esses desafios:

- Implantar vários sites, cada um com seu próprio banco de dados de site SQL Server.

  Esta opção é recomendada para grandes implantações corporativas. Vários sites são gerenciados separadamente, e cada um requer seu próprio banco de dados de site SQL Server. Cada site é uma implantação separada do Citrix Virtual Apps™.

- Configurar várias zonas dentro de um único site.

  A configuração de zonas pode ajudar os usuários em regiões remotas a se conectar a recursos sem necessariamente forçar suas conexões a atravessar grandes segmentos da WAN. O uso de zonas permite o gerenciamento eficaz do site a partir de um único console do Web Studio, Citrix Director e do banco de dados do site. Isso economiza os custos de implantação, pessoal, licenciamento e operação de mais sites contendo bancos de dados separados em locais remotos.

  As zonas podem ser úteis em implantações de todos os tamanhos. Você pode usar zonas para manter aplicativos e desktops mais próximos dos usuários finais, o que melhora o desempenho. Uma zona pode ter um ou mais Controllers instalados localmente para redundância e resiliência, mas isso não é obrigatório.

O número de Controllers configurados no site pode afetar o desempenho de algumas operações, como adicionar novos Controllers ao próprio site. Para evitar isso, recomendamos que você limite o número de zonas em seu site Citrix Virtual Apps ou Citrix Virtual Desktops™ a no máximo 50.

Quando a latência da rede de suas zonas for superior a 250 ms RTT, recomendamos que você implante vários sites em vez de zonas.

Ao longo deste artigo, o termo local refere-se à zona em discussão. Por exemplo, "Um VDA se registra em um Controller local" significa que um VDA se registra em um Controller na zona onde o VDA está localizado.

As zonas nesta versão são semelhantes, mas não idênticas às zonas no XenApp versão 6.5 e anteriores. Por exemplo, nesta implementação de zonas, não há coletores de dados. Todos os Controllers no site se comunicam com um banco de dados do site na zona primária. Além disso, o failover e as zonas preferenciais funcionam de forma diferente nesta versão.

## Tipos de zona

Um site sempre tem uma zona primária. Ele também pode, opcionalmente, ter uma ou mais zonas satélite. As zonas satélite podem ser usadas para recuperação de desastres, data centers geograficamente distantes, filiais, uma nuvem ou uma zona de disponibilidade em uma nuvem.

**Zona primária:**

A zona primária tem o nome padrão "Primary". Esta zona contém o banco de dados do site SQL Server (e servidores SQL de alta disponibilidade, se usados), Web Studio, Director, Citrix StoreFront™, Citrix License Server e Citrix Gateway. Sempre mantenha o banco de dados do site na zona primária.

A zona primária deve ter pelo menos dois Controladores para redundância. A zona primária pode ter VDAs com aplicativos que estão fortemente acoplados ao banco de dados e à infraestrutura.

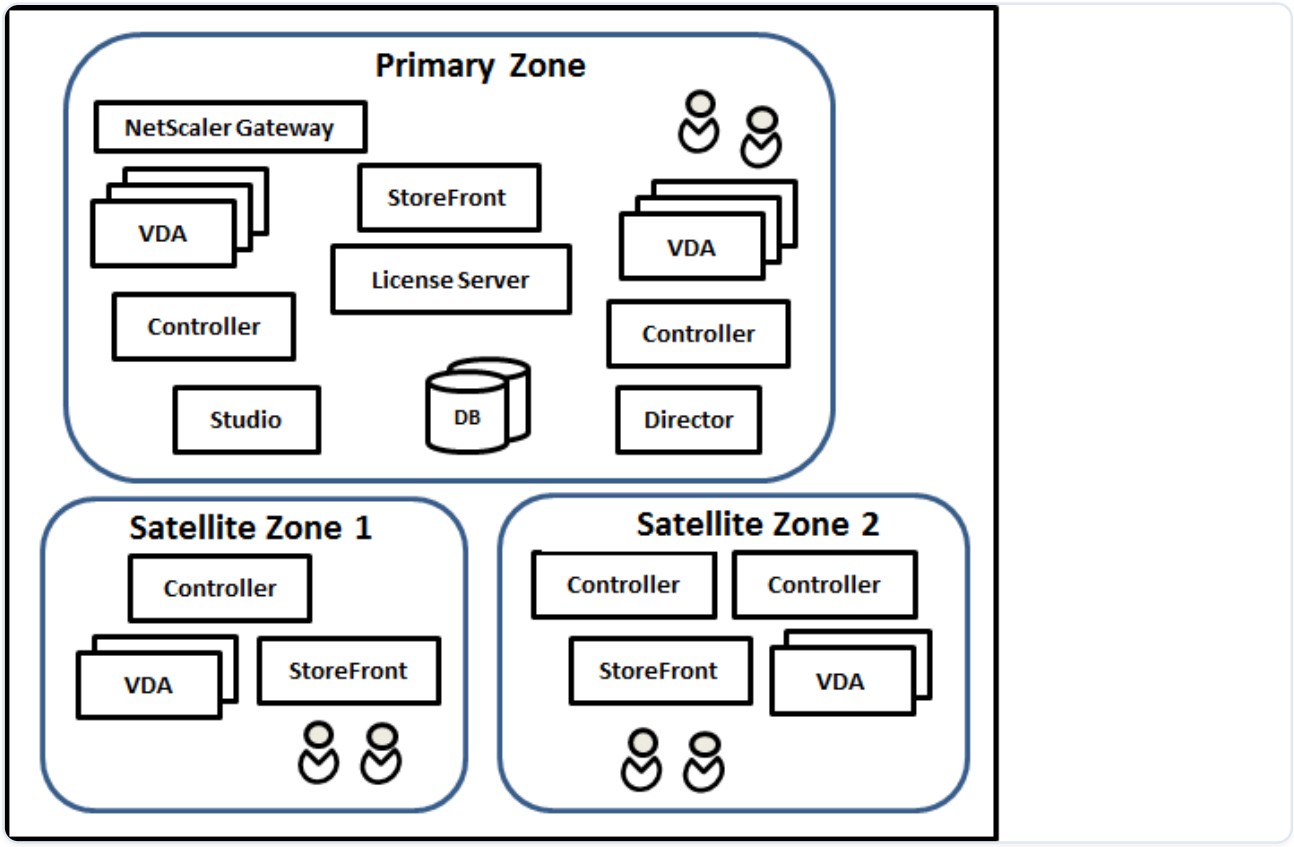
**Zona satélite:**

Uma zona satélite contém um ou mais VDAs, Controladores, servidores StoreFront e servidores Citrix Gateway. Em operações normais, os Controladores em uma zona satélite se comunicam diretamente com o banco de dados na zona primária.

Uma zona satélite, particularmente uma grande, também pode conter um hipervisor que é usado para provisionar e armazenar máquinas para essa zona. Ao configurar uma zona satélite, você

pode associar um hipervisor ou outra conexão de serviço a ela. (Certifique-se de que todos os catálogos que usam essa conexão estejam na mesma zona.)

Um site pode ter zonas satélite com diferentes configurações, com base nas suas necessidades e ambiente exclusivos. A figura a seguir ilustra uma zona primária e exemplos de zonas satélite.




Na ilustração:

- **Zona primária:** Contém dois Controladores, Web Studio, Director, StoreFront, License Server e o banco de dados do site (além de implantações de SQL Server de alta disponibilidade). A zona primária também contém vários VDAs e um Citrix Gateway.
- **Zona satélite 1: VDAs com Controlador:** A zona satélite 1 contém um Controlador, VDAs e um servidor StoreFront. Os VDAs nesta zona satélite se registram no Controlador local. O Controlador local se comunica com o banco de dados do site e o servidor de licenças na zona primária.

  Se a WAN falhar, o recurso Local Host Cache permite que o Controlador na zona satélite continue intermediando conexões com os VDAs nessa zona. Tal implantação pode ser eficaz em um escritório onde os trabalhadores usam um site StoreFront local e o Controlador local para acessar seus recursos locais.

- **Zona satélite 2: VDAs com Controladores redundantes:** A zona satélite 2 contém dois Controladores, VDAs e um servidor StoreFront. Este é o tipo de zona mais resiliente, oferecendo proteção contra uma falha simultânea da WAN e de um dos Controladores locais.

## Onde os VDAs se registram e onde os Controladores fazem failover

Em um site contendo zonas primárias e satélite, com VDAs na versão mínima 7.7:

- Um VDA na zona primária se registra em um Controlador na zona primária. Um VDA na zona primária nunca tenta se registrar em um Controlador em uma zona satélite.
- Um VDA em uma zona satélite se registra em um Controlador local, se possível. (Este é considerado o Controlador preferencial.) Se nenhum Controlador local estiver disponível (por exemplo, porque não podem aceitar mais registros de VDA ou falharam), o VDA tentará se registrar em um Controlador na zona primária. Neste caso, o VDA permanece registrado na zona primária, mesmo que um Controlador em uma zona satélite se torne disponível novamente. Um VDA em uma zona satélite nunca tenta se registrar em um Controlador em outra zona satélite.
- Quando a atualização automática está habilitada para a descoberta de Controladores pelo VDA, e você especifica uma lista de endereços de Controlador durante a instalação do VDA, um Controlador é selecionado aleatoriamente dessa lista para o registro inicial (independentemente da zona em que o Controlador reside). Após a reinicialização da máquina com esse VDA, o VDA começará a preferir registrar-se com um Controlador em sua zona local.
- Se um Controlador em uma zona satélite falhar, ele fará o failover para outro Controlador local, se possível. Se nenhum Controlador local estiver disponível, ele fará o failover para um Controlador na zona primária.
- Se você mover um Controlador para dentro ou para fora de uma zona, e a atualização automática estiver habilitada, os VDAs em ambas as zonas receberão listas atualizadas indicando quais Controladores são locais e quais estão na zona primária, para que saibam com quem podem se registrar e de quem podem aceitar conexões.
- Se você mover um catálogo para outra zona, os VDAs nesse catálogo se registrarão novamente com os Controladores na zona para onde você moveu o catálogo. (Ao mover um catálogo para outra zona, certifique-se de que esta zona e a zona com a conexão de host associada estejam bem conectadas. Se houver largura de banda limitada ou alta latência, mova a conexão de host para a mesma zona que contém o catálogo de máquinas associado.)

Se todos os Controladores na zona primária falharem:

- O Web Studio não consegue se conectar ao site.
- As conexões com VDAs na zona primária não podem ser feitas.
- O desempenho do site degrada até que os Controladores na zona primária estejam disponíveis.

Para sites que contêm versões de VDA anteriores a 7.7:

- Um VDA em uma zona satélite aceita solicitações de Controladores em sua zona local e na zona primária. (VDAs na versão mínima 7.7 podem aceitar solicitações de Controlador de outras zonas satélites.)
- Um VDA em uma zona satélite se registra com um Controlador na zona primária ou na zona local aleatoriamente. (VDAs na versão mínima 7.7 preferem a zona local.)

## Preferência de zona

Para usar o recurso de preferência de zona, você deve estar usando no mínimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

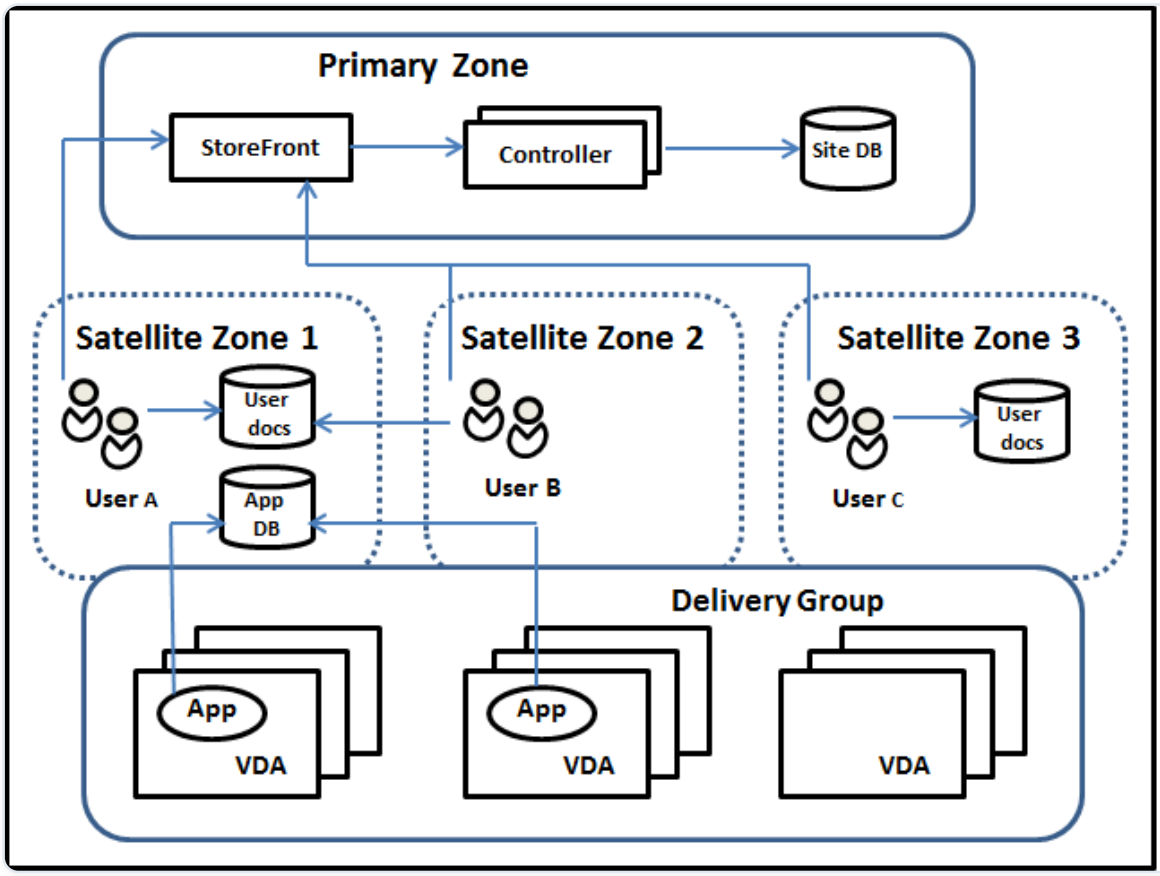
Em um site multi-zona, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou desktop.

### Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma zona específica, com base em:

- Onde os dados do aplicativo são armazenados. Isso é chamado de home do aplicativo.
- O local dos dados home do usuário, como um perfil ou compartilhamento home. Isso é chamado de home do usuário.
- A localização atual do usuário (onde o aplicativo Citrix Workspace™ está sendo executado). Isso é referido como a localização do usuário.

O gráfico a seguir mostra um exemplo de configuração multizona.




Neste exemplo, os VDAs estão espalhados por três zonas satélite, mas todos estão no mesmo Grupo de Entrega. Portanto, o broker pode ter uma escolha de qual VDA usar para uma solicitação de inicialização do usuário. Este exemplo indica que existem vários locais onde os usuários podem estar executando seus endpoints do aplicativo Citrix Workspace:

- O Usuário A está usando um dispositivo com o aplicativo Citrix Workspace na zona satélite 1.
- O Usuário B está usando um dispositivo na zona satélite 2.
- Os documentos de um usuário podem ser armazenados em vários locais.
    - Os Usuários A e B usam um compartilhamento baseado na zona satélite 1.
    - O Usuário C usa um compartilhamento da zona satélite C.
    - Um dos aplicativos publicados usa um banco de dados localizado na zona satélite 1.

Você associa um usuário ou aplicativo a uma zona configurando uma zona inicial para o usuário ou aplicativo. O broker no Delivery Controller™ então usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se houver recursos disponíveis. Você pode:

- Configure a zona home para um usuário adicionando um usuário a uma zona.
- Configure a zona inicial para um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona inicial por vez. (Uma exceção para usuários pode ocorrer quando várias associações de zona ocorrem devido à associação a grupos de usuários; consulte a seção "Outras considerações". No entanto, mesmo neste caso, o broker usa apenas uma zona inicial.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o broker seleciona apenas uma zona preferencial para um lançamento. A ordem de prioridade padrão para selecionar a zona preferencial é zona inicial do aplicativo \> zona inicial do usuário \> localização do usuário. Você pode restringir a sequência; consulte Personalizando a preferência de zona. Quando um usuário inicia um aplicativo:

- Se essa aplicação tiver uma associação de zona configurada (uma zona inicial da aplicação), então a zona preferencial é a zona inicial para essa aplicação.
- Se o aplicativo não tiver uma associação de zona configurada, mas o usuário tiver uma associação de zona configurada (uma zona inicial do usuário), então a zona preferencial é a zona inicial para esse usuário.
- Se nem o aplicativo nem o usuário tiverem uma associação de zona configurada, então a zona preferencial é a zona onde o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, uma seleção aleatória de VDA e zona é usada. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver uma zona preferencial, o balanceamento de carga é aplicado a todos os VDAs no Grupo de Entrega.

### Personalizando a preferência de zona

Ao configurar (ou remover) uma zona inicial para um usuário ou um aplicativo, você também pode restringir ainda mais como a preferência de zona é usada.

- **Uso obrigatório da zona inicial do usuário:** Em um Grupo de Entrega, você pode especificar que as sessões sejam iniciadas na zona inicial do usuário (se configurada), sem failover para outra zona se a zona inicial não tiver recursos disponíveis. Essa restrição é útil quando você precisa evitar o risco de copiar grandes perfis ou arquivos de dados entre zonas. Em outras palavras, você preferiria negar o início de uma sessão a iniciar a sessão em uma zona diferente.
- **Uso obrigatório da zona inicial do aplicativo:** Da mesma forma, ao configurar uma zona inicial para um aplicativo, você pode indicar que o aplicativo seja iniciado somente nessa zona, sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona inicial do aplicativo.

- **Nenhuma zona inicial de aplicativo e ignorar a zona inicial de usuário configurada:** Se você não especificar uma zona inicial para um aplicativo, também poderá indicar que nenhuma zona de usuário configurada seja considerada ao iniciar esse aplicativo. Por exemplo, você pode preferir que os usuários executem um aplicativo em um VDA perto de seu dispositivo, usando a preferência de zona de localização do usuário, mesmo que alguns usuários possam ter uma zona inicial diferente.

### Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia uma aplicação ou desktop, o broker prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário que está iniciando um aplicativo ou desktop já tiver uma sessão adequada para o recurso que está sendo iniciado (por exemplo, que pode usar o compartilhamento de sessão para um aplicativo, ou uma sessão que já está executando o recurso que está sendo iniciado), mas essa sessão estiver sendo executada em um VDA em uma zona diferente da zona preferencial para o usuário/aplicativo, o sistema poderá criar uma nova sessão. Isso satisfaz o lançamento na zona correta (se tiver capacidade disponível), antes de reconectar a uma sessão em uma zona menos preferencial para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não pode mais ser alcançada, a reconexão é permitida para sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem de desejabilidade para as sessões satisfazerem um lançamento é:

1. Reconectar a uma sessão existente na zona preferencial.
2. Reconectar a uma sessão desconectada existente em uma zona diferente da zona preferencial.
3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar a uma sessão existente conectada em uma zona diferente da zona preferencial.
5. Iniciar uma nova sessão em uma zona diferente da zona preferencial.

### Outras considerações sobre a preferência de zona

- Se você configurar uma zona inicial para um grupo de usuários (como um grupo de segurança), os usuários desse grupo (por meio de associação direta ou indireta) serão associados à zona especificada. No entanto, um usuário pode ser membro de vários grupos de segurança e, portanto, pode ter uma zona inicial diferente configurada por meio de outra associação de grupo. Nesses casos, a determinação da zona inicial desse usuário pode ser ambígua.

Se um usuário tiver uma zona inicial configurada que não foi adquirida por meio de associação a grupo, essa zona será usada para preferência de zona. Quaisquer associações de zona adquiridas por meio de associação a grupo são ignoradas.

Se o usuário tiver várias associações de zona diferentes adquiridas exclusivamente por meio da associação a grupos, o broker escolherá aleatoriamente entre as zonas. Uma vez que o broker faça essa escolha, essa zona será usada para lançamentos de sessão subsequentes, até que a associação do usuário ao grupo mude.

- A preferência de zona de localização do usuário requer a detecção do aplicativo Citrix Workspace no dispositivo de endpoint pelo Citrix Gateway através do qual esse dispositivo está se conectando. O Citrix Gateway deve ser configurado para associar intervalos de endereços IP a zonas específicas, e a identidade da zona descoberta deve ser passada pelo StoreFront para o Controller.

Para obter mais informações sobre a preferência de zona, consulte Detalhes internos da preferência de zona.

## Considerações, requisitos e melhores práticas

- Você pode colocar os seguintes itens em uma zona: Controllers, catálogos de máquinas, conexões de host, usuários e aplicativos. Se um catálogo usar uma conexão de host, certifique-se de que o catálogo e a conexão estejam na mesma zona. (No entanto, com uma conexão de baixa latência e alta largura de banda disponível, eles podem estar em zonas diferentes.)
- Quando você coloca itens em uma zona satélite, isso afeta como o site interage com eles e com outros objetos relacionados a eles.
    - Quando os Controllers são colocados em uma zona satélite, presume-se que essas máquinas tenham boa conectividade (local) com hipervisores e VDAs na mesma zona. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária para lidar com esses hipervisores e máquinas VDA.
    - Quando uma conexão de hipervisor é colocada em uma zona satélite, presume-se que todos os hipervisores gerenciados por meio dessa conexão de hipervisor também residam nessa zona satélite. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária ao se comunicar com essa conexão de hipervisor.
    - Quando um catálogo de máquinas é colocado em uma zona satélite, presume-se que todas as máquinas VDA nesse catálogo estejam na zona satélite. Os Controllers locais são usados em preferência aos Controllers na zona primária ao tentar se registrar no site,

depois que o mecanismo de atualização automática da lista de Controllers for ativado após o primeiro registro de cada VDA.

- As instâncias do Citrix Gateway também podem ser associadas a zonas. Isso é feito como parte da configuração de Roteamento HDX™ Otimizado do StoreFront, em vez de, como para os outros elementos descritos aqui, como parte da configuração do site. Quando um Citrix Gateway é associado a uma zona, ele é preferencialmente usado quando conexões HDX para máquinas VDA nessa zona são utilizadas.

- Ao criar um site de produção e, em seguida, criar o primeiro catálogo e Grupo de Entrega, todos os itens estão na zona primária – você não pode criar zonas satélite até concluir essa configuração inicial. (Se você criar um site vazio, a zona primária inicialmente conterá apenas um Controller. Você pode criar zonas satélite antes ou depois de criar um catálogo e um Grupo de Entrega.)
- Ao criar a primeira zona satélite contendo um ou mais itens, todos os outros itens em seu site permanecem na zona primária.
- A zona primária é nomeada 'Primary' por padrão; você pode alterar esse nome. Embora o Web Studio indique qual zona é a zona primária, é uma boa prática usar um nome facilmente identificável para a zona primária. Você pode reatribuir a zona primária (ou seja, tornar outra zona a zona primária), mas ela deve sempre conter o banco de dados do site e quaisquer servidores de alta disponibilidade.
- Sempre mantenha o banco de dados do site na zona primária.
- Depois de criar uma zona, você pode mover itens de uma zona para outra. Essa flexibilidade permite que você separe itens que funcionam melhor em proximidade. Por exemplo, mover um catálogo para uma zona diferente da conexão (host) que cria as máquinas no catálogo pode afetar o desempenho. Considere possíveis efeitos não intencionais antes de mover itens entre zonas. Mantenha um catálogo e a conexão de host que ele usa na mesma zona, ou em zonas bem conectadas (por exemplo, via uma rede de baixa latência e alta largura de banda).
- Para um desempenho ideal, instale o Web Studio e o Director apenas na zona primária. Você pode acessar o Web Studio e o Director de uma zona satélite (por exemplo, uma zona satélite contendo Controllers para usar como failover se a zona primária se tornar inacessível) porque são aplicativos web.
- Idealmente, o Citrix Gateway em uma zona satélite é usado para conexões de usuário que chegam a essa zona de outras zonas ou locais externos, embora você possa usá-lo para conexões dentro da zona.
- Lembre-se: Para usar o recurso de preferência de zona, você deve estar usando no mínimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

### Limites de qualidade da conexão

Os Controllers na zona satélite realizam interações SQL diretamente com o banco de dados do site. Isso impõe alguns limites à qualidade do link entre a zona satélite e a zona primária que contém o banco de dados do site. Os limites específicos são relativos ao número de VDAs e sessões de usuário nesses VDAs que são implantados na zona satélite. Assim, zonas satélite com apenas alguns VDAs e sessões podem funcionar com uma conexão de qualidade inferior ao banco de dados do que zonas satélite com um grande número de VDAs e sessões.

Para obter mais informações, consulte Melhorias na Latência e Bloqueio de Consultas SQL.

### O impacto da latência no desempenho do brokering

Embora as zonas permitam que os usuários estejam em links de maior latência, desde que haja um broker local, a latência adicional inevitavelmente impacta a experiência do usuário final. Para a maioria do trabalho que os usuários realizam, eles experimentam lentidão causada por viagens de ida e volta entre os Controllers na zona satélite e o banco de dados do site.

Para o lançamento de aplicativos, ocorrem atrasos extras enquanto o processo de brokering de sessão identifica VDAs adequados para enviar solicitações de lançamento de sessão.

## Criar e gerenciar zonas

Um Administrador Completo pode realizar todas as tarefas de criação e gerenciamento de zonas. No entanto, você também pode criar uma função personalizada que permite criar, editar ou excluir uma zona. Mover itens entre zonas não requer permissões relacionadas à zona (exceto permissão de leitura da zona); no entanto, você deve ter permissão de edição para os itens que está movendo. Por exemplo, para mover um catálogo de uma zona para outra, você deve ter permissão de edição para esse catálogo. Para obter mais informações, consulte Administração delegada.

**Se você usa Citrix Provisioning™:** O console do Citrix Provisioning não reconhece zonas, por isso recomendamos usar o Web Studio para criar catálogos para zonas satélite. Crie o catálogo no Web Studio, especificando a zona satélite correta. Em seguida, use o console do Citrix Provisioning para provisionar máquinas nesse catálogo. (Se você criar o catálogo usando o assistente do Citrix Provisioning, o catálogo será colocado na zona primária. Você deve usar o Web Studio para movê-lo para a zona satélite posteriormente.)

### Criar uma zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.

3. Selecione **Criar Zona** na barra de ações.
4. Insira um nome para a zona e uma descrição (opcional). O nome deve ser exclusivo dentro do site.
5. Selecione os itens a serem colocados na nova zona. Você pode filtrar ou pesquisar a lista de itens dos quais pode selecionar. Você também pode criar uma zona vazia; simplesmente não selecione nenhum item.
6. Clique em **Salvar**.

Como alternativa a este método, você pode selecionar um ou mais itens no Web Studio e, em seguida, selecionar **Criar Zona** na barra de ações.

### Alterar um nome ou descrição de zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel central e, em seguida, selecione **Editar Zona** na barra de ações.
4. Altere o nome, a descrição ou ambos da zona. Se você alterar o nome da zona primária, certifique-se de que a zona permaneça facilmente identificável como a zona primária.
5. Clique em **Salvar** ou **Aplicar**.

### Mover itens de uma zona para outra zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel do meio e, em seguida, selecione um ou mais itens.
4. Arraste os itens para a zona de destino ou selecione **Mover Itens** na barra de ações e, em seguida, especifique para qual zona movê-los.

Uma mensagem de confirmação lista os itens selecionados e pergunta se você tem certeza de que deseja mover todos eles.

**Lembre-se:** Quando um catálogo usa uma conexão de host com um hipervisor ou outro serviço, coloque o catálogo e a conexão na mesma zona. Caso contrário, o desempenho pode ser afetado. Se você mover um, mova o outro também.

### Excluir uma zona

Uma zona deve estar vazia antes de poder ser excluída. Você não pode excluir a zona primária.

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel central.
4. Selecione **Excluir Zona** na barra de ações. Se a zona não estiver vazia (contiver itens), será solicitado que você escolha a zona para onde esses itens serão movidos.
5. Confirme a exclusão.

### Adicionar uma zona inicial para um usuário

Configurar uma zona inicial para um usuário também é conhecido como *adicionar um usuário a uma zona*.

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo e, em seguida, selecione uma zona no painel central.
3. Selecione **Adicionar Usuários à Zona** na barra de ações.
4. Na caixa de diálogo **Adicionar Usuários à Zona**, clique em **Adicionar** e, em seguida, selecione os usuários e grupos de usuários a serem adicionados à zona. Se você especificar usuários que já têm uma zona inicial, uma mensagem oferece duas opções: **Sim** = adicione apenas os usuários especificados que não têm uma zona inicial; **Não** = retorne à caixa de diálogo de seleção de usuário.
5. Clique em **OK**.

Para usuários com uma zona inicial configurada, você pode exigir que as sessões sejam iniciadas apenas a partir de sua zona inicial:

1. Crie ou edite um grupo de entrega.
2. Na página **Usuários**, selecione a caixa de seleção **Exigir que as sessões sejam iniciadas na zona inicial de um usuário (se configurado)**.

Todas as sessões iniciadas por um usuário nesse grupo de entrega devem ser iniciadas a partir de máquinas na zona inicial desse usuário. Se um usuário no grupo de entrega não tiver uma zona inicial configurada, essa configuração não terá efeito.

### Remover uma zona inicial para um usuário

Este procedimento também é conhecido como remover um usuário de uma zona.

1. Faça logon no Web Studio.
2. Selecione **Zonas** no painel esquerdo e, em seguida, selecione uma zona no painel do meio.

3. Selecione **Remover Usuários da Zona** na barra de ações.
4. Na caixa de diálogo **Adicionar Usuários à Zona**, clique em **Remover** e, em seguida, selecione os usuários e grupos a serem removidos da zona. Esta ação remove os usuários apenas da zona; esses usuários permanecem nos grupos de entrega e grupos de aplicativos aos quais pertencem.
5. Confirme a remoção quando solicitado.

### Gerenciar zonas iniciais para aplicativos

Configurar uma zona inicial para um aplicativo também é conhecido como adicionar um aplicativo a uma zona. Por padrão, em um ambiente multizona, um aplicativo não tem uma zona inicial.

A zona inicial de um aplicativo é especificada nas propriedades do aplicativo. Você pode configurar as propriedades do aplicativo ao adicionar o aplicativo a um grupo ou posteriormente.

- Ao criar um Grupo de Entrega, criar um Grupo de Aplicativos, ou adicionar aplicativos a grupos existentes, selecione **Propriedades** na página **Aplicativos** do assistente.
- Para alterar as propriedades de um aplicativo depois que ele é adicionado, selecione **Aplicativos** no painel esquerdo. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** na barra de ações.

Na página **Zonas** das propriedades/configurações do aplicativo:

- Se você quiser que o aplicativo tenha uma zona inicial:
  - Selecione o botão de opção **Usar a zona selecionada para decidir** e, em seguida, selecione a zona.
  - Se você quiser que o aplicativo seja iniciado apenas da zona selecionada (e não de qualquer outra zona), selecione a caixa de seleção abaixo da seleção de zona.
- Se você não quiser que o aplicativo tenha uma zona inicial:
  - Selecione o botão de opção **Não configurar uma zona inicial**.
  - Se você não quiser que o broker considere nenhuma zona de usuário configurada ao iniciar este aplicativo, selecione a caixa de seleção abaixo do botão de opção. Nesse caso, nem as zonas iniciais de aplicativo nem as de usuário são usadas para determinar onde iniciar este aplicativo.

## Outras ações que incluem a especificação de zonas

Depois de criar pelo menos uma zona satélite, você pode especificar uma zona ao adicionar uma conexão de host ou criar um catálogo.

Geralmente, a zona primária é a padrão. Ao usar o Machine Creation Services™ para criar um catálogo, a zona configurada para a conexão de host é selecionada automaticamente.

Se o site não contiver zonas satélite, a zona primária é assumida e a caixa de seleção de zona não aparece.

# Monitor

Administradores e pessoal de suporte podem monitorar Sites do Citrix Virtual Apps and Desktops™ usando uma variedade de recursos e ferramentas. Usando essas ferramentas, você pode monitorar:

- Sessões de usuário e uso da sessão
- Desempenho de logon
- Conexões e máquinas, incluindo falhas
- Avaliação de carga
- Tendências históricas
- Infraestrutura

## Citrix Director

O Director é uma ferramenta web em tempo real que você pode usar para monitorar e solucionar problemas, e para realizar tarefas de suporte para usuários finais.

Para obter detalhes, consulte os artigos sobre Director.

## Registro de Configuração

O Registro de Configuração permite que os administradores acompanhem as alterações administrativas em um Site. O Registro de Configuração pode ajudar os administradores a diagnosticar e solucionar problemas após a realização de alterações de configuração, auxiliar no gerenciamento de mudanças e rastrear configurações, e relatar a atividade administrativa.

Você pode visualizar e gerar relatórios sobre informações registradas no Studio. Você também pode visualizar itens registrados no Director com a Visualização de Tendências para fornecer notificações de alterações de configuração. Este recurso é útil para administradores que não têm acesso ao Studio.

A Visualização de Tendências fornece dados históricos de alterações de configuração ao longo de um período para que os administradores possam avaliar quais alterações foram feitas no Site,

quando foram feitas e quem as fez para encontrar a causa de um problema. Esta visualização classifica as informações de configuração em três categorias:

- Falhas de Conexão
- Máquinas de sessão única com falha
- Máquinas de múltiplas sessões com falha

Para obter detalhes sobre como habilitar e configurar o Registro de Configuração, consulte Registro de Configuração. Os artigos do Director descrevem como visualizar as informações registradas a partir dessa ferramenta.

## Logs de eventos

Os serviços dentro do Citrix Virtual Apps and Desktops registram os eventos que ocorrem. Os logs de eventos são usados para monitorar e solucionar problemas de operações.

Para obter detalhes, consulte Logs de eventos. Artigos de recursos individuais também podem conter informações de eventos.

## Registro de configuração

O registro de configuração é um recurso que captura as alterações de configuração do site e as atividades administrativas no banco de dados. O recurso é habilitado por padrão. Você pode usar o conteúdo registrado para:

- Diagnosticar e solucionar problemas após a realização de alterações de configuração. O log fornece um rastro de auditoria.
- Auxiliar no gerenciamento de alterações e rastrear configurações.
- Relatar a atividade administrativa.

Você define as preferências de registro de configuração, exibe os logs de configuração e gera relatórios HTML e CSV a partir do Citrix Studio. Você pode filtrar as exibições do log de configuração por intervalos de datas e resultados de pesquisa de texto completo. O registro obrigatório, quando habilitado, impede que alterações de configuração sejam feitas, a menos que possam ser registradas. Com a permissão apropriada, você pode excluir entradas do log de configuração. Você não pode usar o recurso de registro de configuração para editar o conteúdo do log.

O registro de configuração usa um SDK do PowerShell e o Serviço de Registro de Configuração. O Serviço de Registro de Configuração é executado em cada Controller no site. Se um Controller falhar, o serviço em outro Controller lida automaticamente com as solicitações de registro.

Por padrão, o recurso de registro de configuração é habilitado e usa o banco de dados que é criado quando você cria o site (o banco de dados de configuração do site). Você pode especificar um local diferente para o banco de dados. O banco de dados de registro de configuração suporta os mesmos recursos de alta disponibilidade que o banco de dados de configuração do site.

O acesso ao registro de configuração é controlado por meio de administração delegada, com as permissões Editar Preferências de Registro e Visualizar Logs de Configuração.

Os logs de configuração são localizados quando são criados. Por exemplo, um log criado em inglês é lido em inglês, independentemente da localidade do leitor.

## O que é registrado

Alterações de configuração e atividades administrativas iniciadas a partir do Studio, Director e scripts do PowerShell são registradas. Exemplos de alterações de configuração registradas incluem trabalhar com (criar, editar, excluir, atribuir):

- Catálogos de máquinas
- Grupos de entrega (incluindo a alteração das configurações de gerenciamento de energia)
- Funções e escopos de administrador
- Recursos e conexões de host
- Políticas Citrix através do Studio

Exemplos de alterações administrativas registradas incluem:

- Gerenciamento de energia de uma máquina virtual ou de um desktop de usuário
- Studio ou Director enviando uma mensagem a um usuário

As seguintes operações não são registradas:

- Operações autônomas, como o ligamento de máquinas virtuais pelo gerenciamento de pool.
- Ações de política implementadas por meio do Console de Gerenciamento de Política de Grupo (GPMC); use ferramentas da Microsoft para visualizar os logs dessas ações.
- Alterações feitas por meio do registro, acesso direto ao banco de dados ou de fontes diferentes de Studio, Director ou PowerShell.

- Quando a implantação é inicializada, o registro de configuração fica disponível quando a primeira instância do Serviço de Registro de Configuração se registra no Serviço de Configuração. Portanto, os estágios iniciais da configuração não são registrados (por exemplo, quando o esquema do banco de dados é obtido e aplicado, quando um hipervisor é inicializado).

## Gerenciar o registro de configuração

Por padrão, o registro de configuração usa o banco de dados criado ao criar um site (também conhecido como banco de dados de configuração do site). A Citrix recomenda que você use um local separado para o banco de dados de registro de configuração (e o banco de dados de monitoramento) pelos seguintes motivos:

- A estratégia de backup para o banco de dados de registro de configuração provavelmente difere da estratégia de backup para o banco de dados de configuração do site.
- O volume de dados coletados para o registro de configuração (e o Serviço de Monitoramento) pode afetar negativamente o espaço disponível para o banco de dados de configuração do site.
- Isso divide o ponto único de falha para os três bancos de dados.

As edições do produto que não suportam o registro de configuração não possuem um nó de Registro no Studio.

## Habilitar e desabilitar o registro de configuração e o registro obrigatório

Por padrão, o registro de configuração está ativado e o registro obrigatório está desativado.

1. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
2. Selecione **Preferências** na barra de ações. A caixa de diálogo de registro de configuração contém informações do banco de dados e indica se o registro de configuração e o registro obrigatório estão ativados ou desativados.
3. Selecione a ação desejada:

   Para ativar o registro de configuração, selecione **Ativar**. Esta é a configuração padrão. Se o banco de dados não puder ser gravado, as informações de registro serão descartadas, mas a operação continuará.

   Para desativar o registro de configuração, selecione **Desativar**. Se o registro estava ativado anteriormente, os logs existentes permanecem legíveis com o SDK do PowerShell.

Para ativar o registro obrigatório, selecione **Impedir alterações na configuração do site quando o banco de dados não estiver disponível**. Nenhuma alteração de configuração ou atividade administrativa que é normalmente registrada é permitida, a menos que possa ser gravada no banco de dados de registro de configuração. Você pode ativar o registro obrigatório somente quando o registro de configuração estiver ativado (quando **Ativar** for selecionado). Se o Serviço de Registro de Configuração falhar e a alta disponibilidade não estiver em uso, o registro obrigatório será assumido. Nesses casos, as operações que normalmente seriam registradas não são executadas.

Para desativar o registro obrigatório, selecione **Permitir alterações na configuração do site quando o banco de dados não estiver disponível**. Alterações de configuração e atividades administrativas são permitidas, mesmo que o banco de dados de registro de configuração não possa ser acessado. Esta é a configuração padrão.

## Alterar o local do banco de dados de registro de configuração

Você não pode alterar o local do banco de dados quando o registro obrigatório está ativado, porque a alteração de local inclui um breve intervalo de desconexão que não pode ser registrado.

1. Crie um servidor de banco de dados, usando uma versão suportada do SQL Server.
2. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
3. Selecione **Preferências** na barra de ações.
4. Na caixa de diálogo Preferências de Registro, selecione **Alterar banco de dados de registro**.
5. Na caixa de diálogo Alterar Banco de Dados de Registro, especifique o local do servidor que contém o novo servidor de banco de dados. Consulte Formatos de endereço de banco de dados para formatos válidos.
6. Para permitir que o Studio crie o banco de dados, clique em **OK**. Quando solicitado, clique em **OK**, e ele será criado automaticamente. O Studio tenta acessar o banco de dados usando as credenciais do usuário atual do Studio. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. Em seguida, o Studio carrega o esquema do banco de dados para ele. (As credenciais são retidas apenas durante a criação do banco de dados.)
7. Para criar o banco de dados manualmente, clique em **Gerar script do banco de dados**. O script gerado inclui instruções para criar o banco de dados manualmente. Certifique-se de que o banco de dados esteja vazio e que pelo menos um usuário tenha permissão para acessar e alterar o banco de dados antes de carregar o esquema.

Os dados de log de configuração do banco de dados anterior não são importados para o novo banco de dados. Os logs não podem ser agregados de ambos os bancos de dados ao recuperá-

los. A primeira entrada de log no novo banco de dados de log de configuração indica que uma alteração no banco de dados ocorreu, mas não identifica o banco de dados anterior.

## Exibir conteúdo do log de configuração

Ao iniciar alterações de configuração e atividades administrativas, as operações de alto nível criadas pelo Studio e Director são listadas no painel superior central do Studio. Uma operação de alto nível resulta em uma ou mais chamadas de serviço e SDK, que são operações de baixo nível. Ao selecionar uma operação de alto nível no painel superior, o painel inferior exibe as operações de baixo nível.

Se uma operação falhar antes da conclusão, a operação de log pode não ser concluída no banco de dados. Por exemplo, um registro de início não terá um registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Ao exibir logs com base em intervalos de tempo, logs incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se todos os logs dos últimos cinco dias forem solicitados e um log existir com um horário de início nos últimos cinco dias, mas não tiver um horário de término, ele será incluído.

Ao usar um script que chama cmdlets do PowerShell, se você criar uma operação de baixo nível sem especificar uma operação de alto nível pai, o log de configuração criará uma operação de alto nível substituta.

Para exibir o conteúdo do log de configuração, selecione **Registro** no painel de navegação do Studio. Por padrão, o painel central lista o conteúdo do log cronologicamente (entradas mais recentes primeiro), separado por data. Você pode:

- Classificar a exibição pelo cabeçalho da coluna.
- Filtrar a exibição especificando um intervalo de dias ou inserindo texto na caixa **Pesquisar**. Para retornar à exibição padrão após usar a pesquisa, limpe o texto na caixa **Pesquisar**.

## Gerar relatórios

Você pode gerar relatórios CSV e HTML contendo dados de log de configuração.

- O relatório CSV contém todos os dados de log de um intervalo de tempo especificado. Os dados hierárquicos no banco de dados são nivelados em uma única tabela CSV. Nenhum aspecto dos dados tem precedência no arquivo. Nenhuma formatação é usada e nenhuma legibilidade humana é assumida. O arquivo (nomeado MyReport) contém os dados em um formato universalmente consumível. Arquivos CSV são frequentemente usados para arquivar dados ou como fonte de dados para uma ferramenta de relatório ou manipulação de dados, como o Microsoft Excel.

- O relatório HTML fornece uma forma legível por humanos dos dados de log para um intervalo de tempo especificado. Ele fornece uma visualização estruturada e navegável para revisar as alterações. Um relatório HTML compreende dois arquivos, nomeados Resumo e Detalhes. O Resumo lista as operações de alto nível: quando cada operação ocorreu, por quem e o resultado. Clicar em um link **Detalhes** ao lado de cada operação leva você às operações de baixo nível no arquivo Detalhes, que fornece informações adicionais.

Para gerar um relatório de log de configuração, selecione **Registro** no painel de navegação do Studio e, em seguida, selecione **Criar relatório personalizado** na barra de ações.

- Selecione o intervalo de datas para o relatório.
- Selecione o formato do relatório: CSV, HTML ou ambos.
- Navegue até o local onde você deseja salvar o relatório.

## Excluir conteúdo do log de configuração

Para excluir o log de configuração, você deve ter certas permissões de administração delegada e de banco de dados SQL Server.

- **Administração delegada:** Você deve ter uma função de administração delegada que permita a leitura da configuração da implantação. A função de administrador completo tem essa permissão. Uma função personalizada deve ter Somente Leitura ou Gerenciar selecionado na categoria Outras permissões.

  Para criar um backup dos dados de log de configuração antes de excluí-los, a função personalizada também deve ter Somente Leitura ou Gerenciar selecionado na categoria Permissões de Log.
- **Banco de dados SQL Server:** Você deve ter um login de servidor SQL com permissão para excluir registros do banco de dados. Existem duas maneiras de fazer isso:
  - Use um login de banco de dados SQL Server com uma função de servidor sysadmin, que permite realizar qualquer atividade no servidor de banco de dados. Alternativamente, as funções de servidor `serveradmin` ou `setupadmin` permitem realizar operações de exclusão.
  - Se sua implantação exigir mais segurança, use um login de banco de dados não-sysadmin mapeado para um usuário de banco de dados que tenha permissão para excluir registros do banco de dados.

    a. No SQL Server Management Studio, crie um login do SQL Server com uma função de servidor diferente de 'sysadmin'.

b. Mapeie o login para um usuário no banco de dados. O SQL Server cria automaticamente um usuário no banco de dados com o mesmo nome do login.

c. Na associação de função de banco de dados, especifique pelo menos um dos membros da função para o usuário do banco de dados: `ConfigurationLoggingSchema_ROLE` ou `dbowner`.

Para obter mais informações, consulte a documentação do SQL Server Management Studio.

Para excluir os logs de configuração:

1. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
2. Selecione **Excluir logs** na barra de ações.
3. É perguntado se você deseja criar um backup dos logs antes que eles sejam excluídos. Se você optar por criar um backup, navegue até o local onde o arquivo de backup será salvo. O backup é criado como um arquivo CSV.

Depois que os logs de configuração são limpos, a exclusão do log é a primeira atividade publicada no log vazio. Essa entrada fornece detalhes sobre quem excluiu os logs e quando.

## Exibir logs de API e PowerShell

Para monitorar as solicitações de API feitas durante sua sessão atual, clique na guia **APIs**. Os logs de API são limpos depois que você sai do Web Studio.

Para exibir os comandos do PowerShell correspondentes às ações da interface do usuário que você realizou durante o dia, clique na guia **PowerShell**.

## Associar metadados a logs de configuração

Você pode anexar metadados a logs de configuração associando um par `name-value` chamado `MetadataMap` aos registros de log.

> **Observação:**
>
> - Você só pode anexar metadados a objetos de operação de alto nível.
> - Os metadados são associados aos registros existentes no momento da execução.

### Definir os metadados

Execute o comando PowerShell `Set-LogHighLevelOperationMetadata` para associar um registro de log ao `MetadataMap`. `Set-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**: ID da operação de alto nível.
- **InputObject**: As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id`, onde um objeto de operação de alto nível ou uma lista de objetos é passado para o comando PowerShell.
- **Nome**: Nome da propriedade dos metadados a serem adicionados. A propriedade deve ser exclusiva para a operação de alto nível especificada. A propriedade não pode conter nenhum dos seguintes caracteres ()\/;:#.*?=<>|'".
- **Valor**: Valor para a propriedade.
- **Mapa**: Dicionário de pares (nome, valor) para as propriedades. Esta é uma alternativa para definir os metadados usando os parâmetros `-Name` e `-Value`.

Por exemplo, para anexar os metadados a todos os registros de log de alto nível com Id 40, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

Para anexar os metadados ao registro de alto nível com o usuário `abc@example.com`, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

### Recuperar usando os metadados

Execute os seguintes comandos PowerShell para usar os metadados associados para recuperar os registros de log:

- Pesquisar por chave e valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Pesquisar por valor qualquer chave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Pesquisar por chave e qualquer valor:

```
Get-LogHighLevelOperation -Metadata "Key:*"
```

### Remover os metadados

Execute o comando PowerShell `Remove-LogHighLevelOperationMetadata` para remover os metadados associados. `Remove-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**: ID da operação de alto nível.
- **InputObject**: As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id``, onde um objeto de operação de alto nível ou uma lista de objetos é passado para o comando PowerShell.
- **Nome**: Nome da propriedade dos metadados a serem removidos. Defina como $null para remover todos os metadados para o objeto especificado.
- **Mapa**: Dicionário de pares (nome, valor) para as propriedades. Isso pode ser uma hashtable (criada com @{"name1" = "val1"; "name2" = "val2"}) ou um dicionário de strings (criado com new-object "System.Collections.Generic.Dictionary"). As propriedades cujos nomes correspondem às chaves no mapa são removidas.

## Logs de eventos

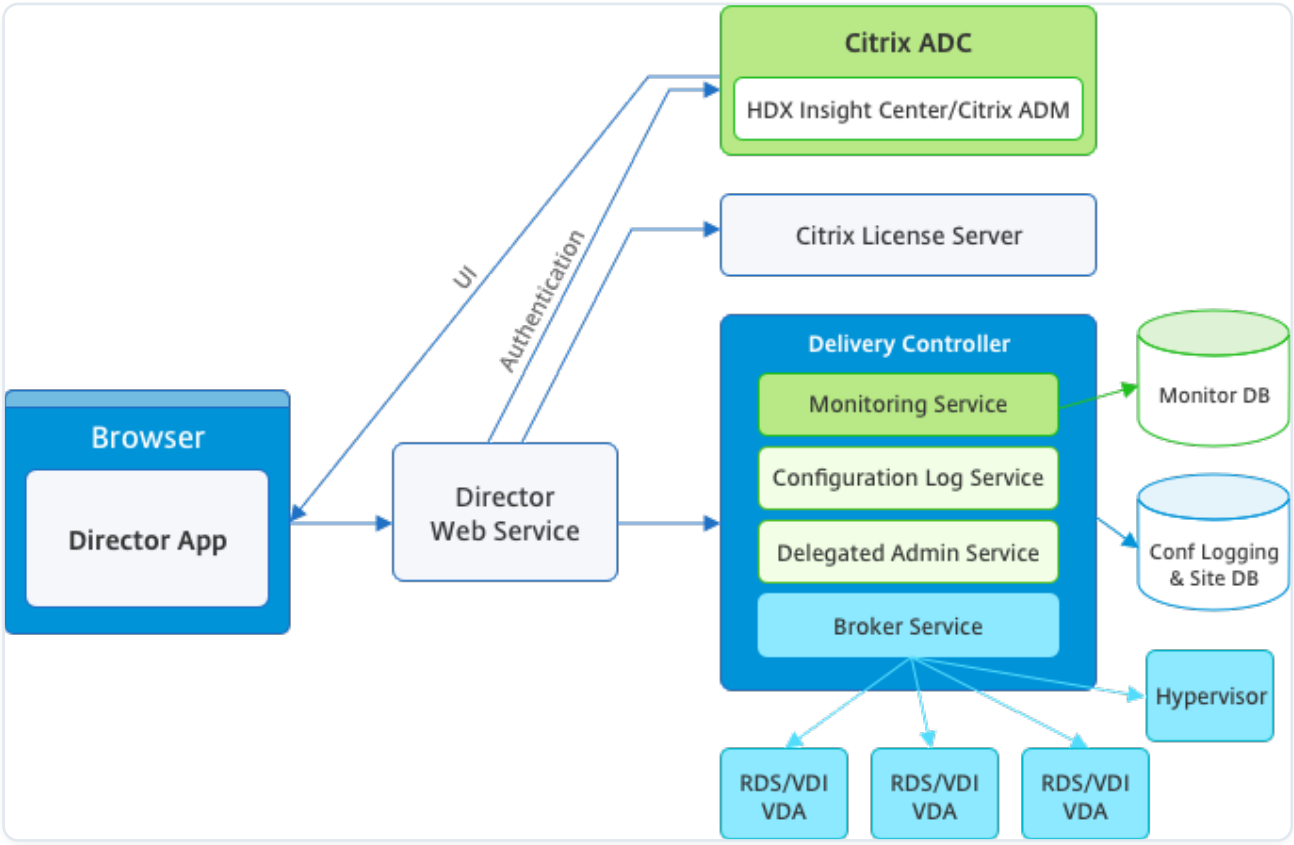
Os artigos a seguir listam e descrevem eventos que podem ser registrados pelos serviços no Citrix Virtual Apps and Desktops.

Esta informação não é abrangente. Os leitores devem verificar os artigos de recursos individuais para obter informações adicionais sobre eventos.

- Eventos do Citrix Broker Service(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/downloads/broker_events.htm)
- Eventos do SDK do Citrix FMA Service(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/downloads/service_core_events.htm)
- Eventos do Citrix Configuration Service(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/downloads/configuration_events.htm)
- Eventos do Citrix Delegated Administration Service(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/downloads/delegated_admin_events.htm)

# Director

O Director é um console de monitoramento e solução de problemas para Citrix Virtual Apps and Desktops.




O Director pode acessar:

- Dados em tempo real do Broker Agent usando um console unificado integrado com Analytics, Performance Manager e Network Inspector. As seguintes análises são fornecidas pelo Citrix ADM para identificar gargalos devido à rede em seu ambiente Citrix Virtual Apps™ ou Desktops:
  - Gerenciamento de desempenho para garantia de integridade e capacidade
  - Tendências históricas e análise de rede
- Dados históricos armazenados no banco de dados Monitor para acessar o banco de dados Configuration Logging.
- Dados ICA® do Citrix Gateway usando o Citrix ADM.

- Obtenha visibilidade da experiência do usuário final para aplicativos virtuais, desktops e usuários para Citrix Virtual Apps ou Desktops.
- Correlacione dados de rede com dados de aplicativos e métricas em tempo real para uma solução de problemas eficaz.
- Integre-se com a ferramenta de monitoramento Citrix Virtual Desktop 7 Director.

O Director usa um painel de solução de problemas que fornece monitoramento de integridade em tempo real e histórico do Site do Citrix Virtual Apps ou Desktops. Esse recurso permite que você veja falhas em tempo real, fornecendo uma ideia melhor do que os usuários finais estão experimentando.

Para obter mais informações sobre a compatibilidade dos recursos do Director com o Delivery Controller (DC), VDA e quaisquer outros componentes dependentes, consulte Matriz de compatibilidade de recursos.

> **Observação:**

> Com a divulgação das vulnerabilidades de canal lateral de execução especulativa Meltdown e Spectre, a Citrix recomenda que você instale os patches de mitigação relevantes. Esses patches podem afetar o desempenho do SQL Server. Para obter mais informações, consulte o artigo de suporte da Microsoft, Proteja o SQL Server contra ataques a vulnerabilidades de canal lateral Spectre e Meltdown. A Citrix recomenda que você teste a escala e planeje suas cargas de trabalho antes de implementar os patches em seus ambientes de produção.

> O Director é instalado por padrão como um site no Delivery Controller. Para pré-requisitos e outros detalhes, consulte a documentação Requisitos do sistema para esta versão. Para informações específicas sobre a instalação e configuração do Director, consulte Instalar e configurar o Director.

# Fazer logon no Director

O site do Director está em https ou `http://<Server FQDN>/Director`.

Se um dos Sites em uma implantação multi-site estiver inativo, o logon demorará um pouco mais enquanto tenta se conectar ao Site que está inativo.

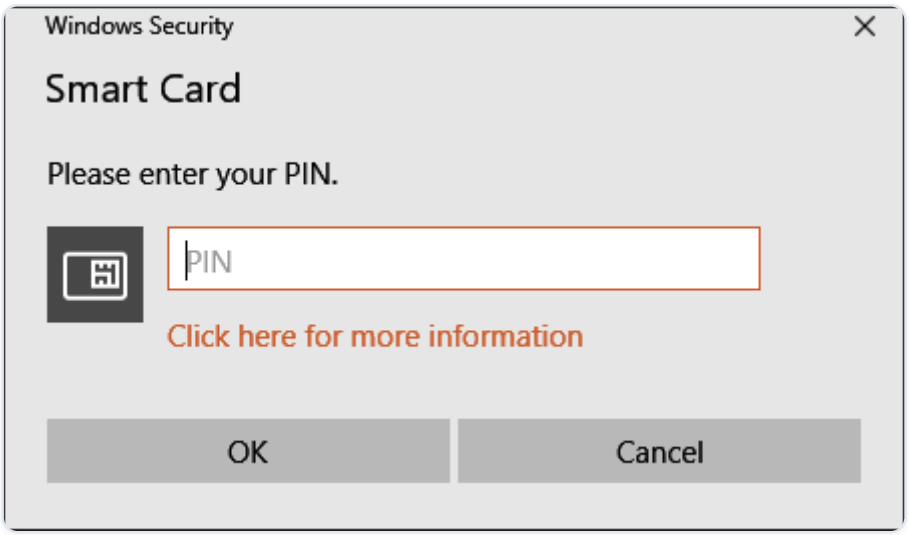
# Usar o Director com autenticação de cartão inteligente PIV

O Director agora oferece suporte à autenticação de cartão inteligente baseada em Verificação de Identidade Pessoal (PIV) para fazer logon. Esse recurso é útil para organizações e agências governamentais que usam autenticação baseada em cartão inteligente para controle de acesso. A autenticação de cartão inteligente requer configuração específica no servidor Director e no Active Directory. As etapas de configuração são detalhadas em Configurar a autenticação de cartão inteligente PIV.

> **Observação:**
>
> A autenticação de cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

Após realizar a configuração necessária, você pode fazer logon no Director usando um cartão inteligente:

1. Insira seu cartão inteligente no leitor de cartão inteligente.
2. Abra um navegador e acesse a URL do Director, `https://<directorfqdn>/Director`.
3. Selecione um certificado de usuário válido na lista exibida.
4. Insira seu token de cartão inteligente.




5. Após a autenticação, você pode acessar o Director sem inserir credenciais adicionais na página de logon do Director.

# Usar o Director com autenticação integrada do Windows

Com a Autenticação Integrada do Windows (IWA), usuários ingressados no domínio obtêm acesso direto ao Director sem precisar digitar novamente suas credenciais na página de logon do Director. Os pré-requisitos para trabalhar com a Autenticação Integrada do Windows e o Director são:

- Habilite a Autenticação Integrada do Windows no site do IIS que hospeda o Director. Ao instalar o Director, as Autenticações Anônima e de Formulários são habilitadas. Para oferecer suporte à Autenticação Integrada do Windows e ao Director, desabilite a Autenticação Anônima e habilite a Autenticação do Windows. A Autenticação de Formulários deve permanecer definida como Habilitada para a autenticação de usuários não-domínio.

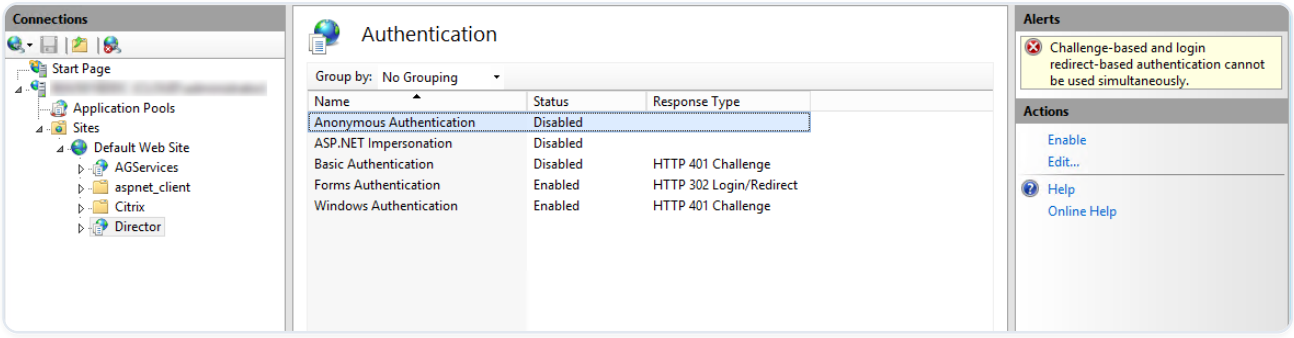
  a. Inicie o gerenciador do IIS.

  b. Vá para **Sites** \> **Default Web Site** \> **Director**.

  c. Selecione **Autenticação**.

  d. Clique com o botão direito em **Autenticação Anônima** e selecione **Desabilitar**.

  e. Clique com o botão direito em **Autenticação do Windows** e selecione **Habilitar**.




- Configure a permissão de delegação do Active Directory para a máquina do Director. A configuração é necessária apenas se o Director e o Delivery Controller™ estiverem instalados em máquinas separadas.

  a. Na máquina do Active Directory, abra o Console de Gerenciamento do Active Directory.

  b. No Console de Gerenciamento do Active Directory, navegar para **Nome do Domínio** \> **Computadores.** Selecione a máquina do Director.

  c. Clique com o botão direito e selecione **Propriedades**.

  d. Em Propriedades, selecione a guia **Delegação**.

  e. Selecione a opção, **Confiar neste computador para delegação a qualquer serviço (somente Kerberos)**.

- O navegador usado para acessar o Director deve suportar a Autenticação Integrada do Windows. Etapas de configuração adicionais podem ser necessárias no Firefox e no Chrome. Para obter mais informações, consulte a documentação do navegador.
- O Serviço de Monitoramento deve estar executando o Microsoft .NET Framework 4.5.1 ou uma versão posterior compatível listada nos Requisitos do Sistema para o Director. Para obter mais informações, consulte Requisitos do Sistema.

Quando um usuário faz logoff do Director ou se a sessão expira, a página de logon é exibida. Na página de logon, o usuário pode definir o tipo de autenticação para **Logon automático** ou **Credenciais do usuário**.

## Visualizações da interface

O Director oferece diferentes visualizações da interface adaptadas a administradores específicos. As permissões do produto determinam o que é exibido e os comandos disponíveis.

Por exemplo, os administradores de help desk veem uma interface adaptada às tarefas de help desk. O Director permite que os administradores de help desk pesquisem o usuário que relata um problema e exibam a atividade associada a esse usuário. Por exemplo, o status dos aplicativos e processos do usuário. Eles podem resolver problemas rapidamente executando ações como encerrar um aplicativo ou processo que não responde, operações de sombreamento na máquina do usuário, reiniciar a máquina ou redefinir o perfil do usuário.

Em contraste, os administradores completos veem e gerenciam todo o Site e podem executar comandos para vários usuários e máquinas. O Painel fornece uma visão geral dos principais aspectos de uma implantação, como o status das sessões, logons de usuários e a infraestrutura do Site. As informações são atualizadas a cada minuto. Se ocorrerem problemas, os detalhes sobre o número e o tipo de falhas que ocorreram aparecerão automaticamente.

Para obter mais informações sobre as várias funções e suas permissões no Director, consulte Administração Delegada e Director

## Coleta de dados de uso pelo Google Analytics

O Serviço Director começa a usar o Google Analytics para coletar dados de uso após a instalação do Director. São coletadas estatísticas sobre o uso das páginas de Tendências e análises de chamadas da API OData. A coleta de análises está em conformidade com a Política de Privacidade da Citrix. A coleta de dados é habilitada por padrão ao instalar o Director.

Para desativar a coleta de dados do Google Analytics, edite a chave do Registro na máquina onde o Director está instalado. Se a chave do Registro não existir, crie-a e defina-a para o valor desejado. Atualize a instância do Director após alterar o valor da chave do Registro.

**Cuidado:** O uso incorreto do Editor do Registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

Local: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGoogleAnalytics

Valor: 0 = ativado (padrão), 1 = desativado

Você pode usar o seguinte cmdlet do PowerShell para desativar a coleta de dados pelo Google Analytics:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

# Guia de novos recursos

O Director possui um guia no produto que usa Pendo para fornecer uma visão sobre os novos recursos lançados na versão atual do Director. A visão geral rápida, juntamente com mensagens apropriadas no produto, ajuda você a entender as novidades do produto.

Para desativar este recurso, edite a chave do registro, conforme descrito abaixo na máquina onde o Director está instalado. Se a chave do registro não existir, crie-a e defina-a para o valor desejado. Atualize a instância do Director após alterar o valor da chave do registro.

> **Cuidado:**

> O uso incorreto do Editor do Registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas

> resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

> Local: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGuidedHelp

Valor: 0 = ativado (padrão), 1 = desativado

Você pode usar o seguinte cmdlet do PowerShell para desativar o guia no produto:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

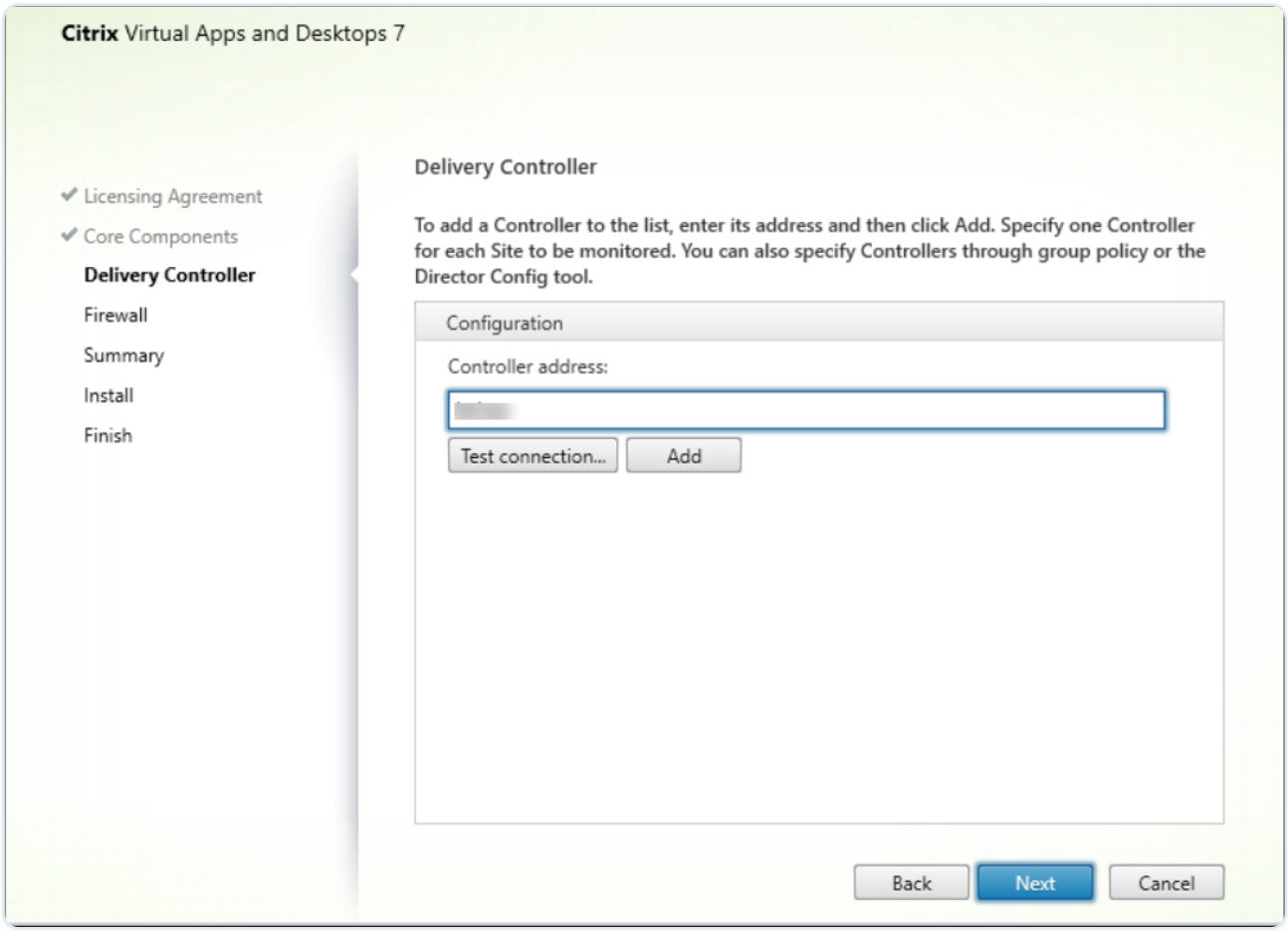
# Instalar e configurar

## Instalar o Director

Instale o Director usando o Instalador ISO completo do produto para Citrix Virtual Apps and Desktops, que verifica os pré-requisitos, instala quaisquer componentes ausentes, configura o site do Director e executa a configuração básica. Para pré-requisitos e outros detalhes, consulte a documentação de Requisitos do sistema para esta versão. Esta versão do Director não é compatível com implantações do Virtual Apps anteriores à 6.5 ou implantações do Virtual Desktops anteriores à 7. A configuração padrão fornecida pelo instalador ISO lida com implantações típicas. Se o Director não foi incluído durante a instalação, use o instalador ISO para adicionar o Director. Para adicionar quaisquer componentes adicionais, execute novamente o instalador ISO e selecione os componentes a serem instalados. Para obter informações sobre como usar o instalador ISO, consulte Instalar componentes principais na documentação de instalação. A Citrix recomenda que você instale usando apenas o instalador ISO completo do produto, e não o arquivo .MSI.

Quando o Director é instalado no Controller, ele é configurado automaticamente com localhost como endereço do servidor, e o Director se comunica com o Controller local por padrão. Para

instalar o Director em um servidor dedicado que esteja remoto de um Controller, você será solicitado a inserir o FQDN ou o endereço IP de um Controller.




**Observação:**

Clique em **Adicionar** para adicionar o Controller a ser monitorado.

O Director se comunica com o Controller especificado por padrão. Especifique apenas um endereço de Controller para cada site que você monitora. O Director descobre automaticamente todos os outros Controllers no mesmo site e recorre a esses outros Controllers se o Controller especificado falhar.

**Observação:**

O Director não faz balanceamento de carga entre os Controllers.

Para proteger as comunicações entre o navegador e o servidor Web, a Citrix® recomenda que você implemente TLS no site do IIS que hospeda o Director. Consulte a documentação do Microsoft IIS para obter instruções. A configuração do Director não é necessária para habilitar o TLS.

## Implantar e configurar o Director

Quando o Director é usado em um ambiente que contém mais de um site, certifique-se de sincronizar os relógios do sistema em todos os servidores onde os Controllers, o Director e outros componentes principais estão instalados. Caso contrário, os sites podem não ser exibidos corretamente no Director.

**Importante:**

Para proteger a segurança de nomes de usuário e senhas enviados em texto simples pela rede, permita conexões do Director usando apenas HTTPS, e não HTTP. Certas ferramentas são capazes de ler nomes de usuário e senhas em texto simples em pacotes de rede HTTP (não criptografados), o que pode criar um risco potencial de segurança para os usuários.

### Configurar permissões

Para fazer logon no Director, os administradores com permissões para o Director devem ser usuários de domínio do Active Directory e devem ter os seguintes direitos:

- Direitos de leitura em todas as florestas do Active Directory a serem pesquisadas (consulte Configuração avançada).
- Funções de Administrador Delegado configuradas (consulte administração delegada e Director).
- Para fazer sombra em usuários, os administradores devem ser configurados usando uma política de grupo da Microsoft para Assistência Remota do Windows. Além disso:
    - Ao instalar VDAs, certifique-se de que o recurso Assistência Remota do Windows esteja habilitado em todos os dispositivos de usuário (selecionado por padrão).
    - Ao instalar o Director em um servidor, certifique-se de que a Assistência Remota do Windows esteja instalada (selecionada por padrão). No entanto, ela é desabilitada no servidor por padrão. O recurso não precisa ser habilitado para que o Director forneça assistência aos usuários finais. A Citrix recomenda deixar o recurso desabilitado para melhorar a segurança no servidor.

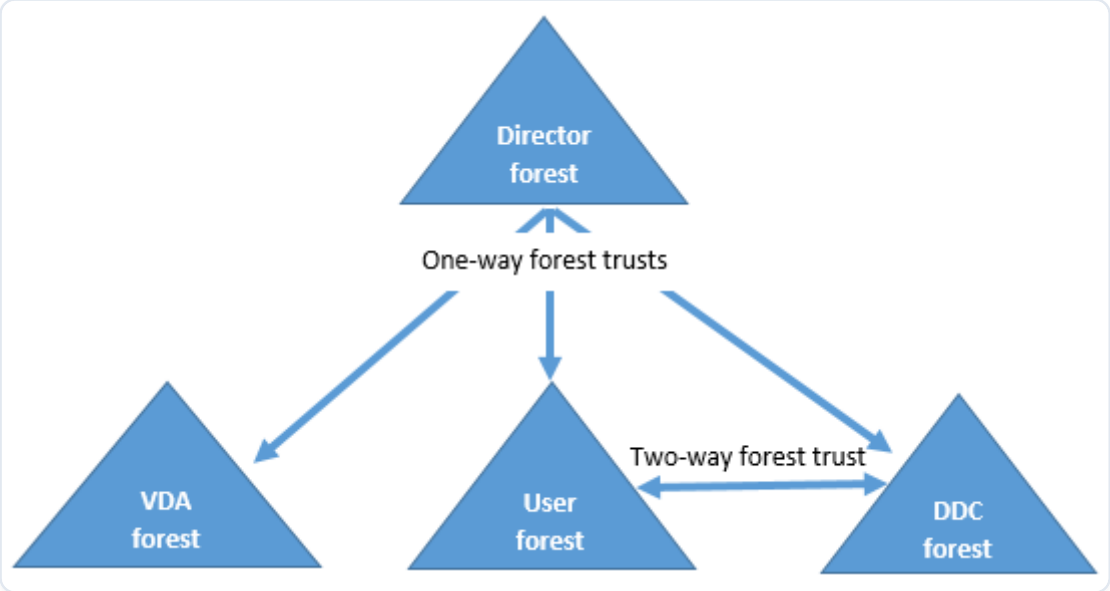
- Para permitir que os administradores iniciem a Assistência Remota do Windows, conceda a eles as permissões necessárias usando as configurações apropriadas da Política de Grupo da Microsoft para Assistência Remota. Para obter informações, consulte CTX127388: How to Enable Remote Assistance for Desktop Director.

## Configuração avançada

O Director pode suportar ambientes multiflorestas abrangendo uma configuração de floresta onde usuários, Delivery Controllers (DCs), VDAs e Directors estão localizados em florestas diferentes. Isso requer uma configuração adequada de relações de confiança entre as florestas e configurações.

### Configuração recomendada em um ambiente multifloresta

A configuração recomendada requer a criação de relações de confiança de floresta de saída e de entrada entre as florestas com autenticação em todo o domínio.




A relação de confiança do Director permite solucionar problemas em sessões de usuário, VDAs e Delivery Controllers localizados em florestas diferentes.

A configuração avançada necessária para o Director suportar várias florestas é controlada por meio de configurações definidas no Gerenciador de Serviços de Informações da Internet (IIS).

> **Importante:**
>
> Ao alterar uma configuração no IIS, o serviço Director é reiniciado automaticamente e desconecta os usuários.

> Para configurar as configurações avançadas usando o IIS:

1. Abra o console do Gerenciador de Serviços de Informações da Internet (IIS).
2. Vá para o site do Director em Site Padrão.
3. Clique duas vezes em **Configurações do Aplicativo**.
4. Clique duas vezes em uma configuração para editá-la.
5. Clique em **Adicionar** para adicionar uma nova configuração.

O Director usa o Active Directory para pesquisar usuários e para procurar mais informações de usuário e máquina. Por padrão, o Director pesquisa o domínio ou floresta em que:

- A conta do administrador é um membro.
- O servidor web do Director é um membro (se diferente).

O Director tenta realizar pesquisas no nível da floresta usando o catálogo global do Active Directory. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

Pesquisar ou consultar dados de outro domínio ou floresta do Active Directory exige que você defina explicitamente os domínios ou florestas a serem pesquisados. Configure a seguinte configuração de Aplicativos para o site do Director no Gerenciador do IIS:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Os atributos de valor user e server representam os domínios do usuário do Director (o administrador) e do servidor do Director, respectivamente.

Para habilitar pesquisas de um domínio ou floresta extra, adicione o nome do domínio à lista, conforme mostrado neste exemplo:

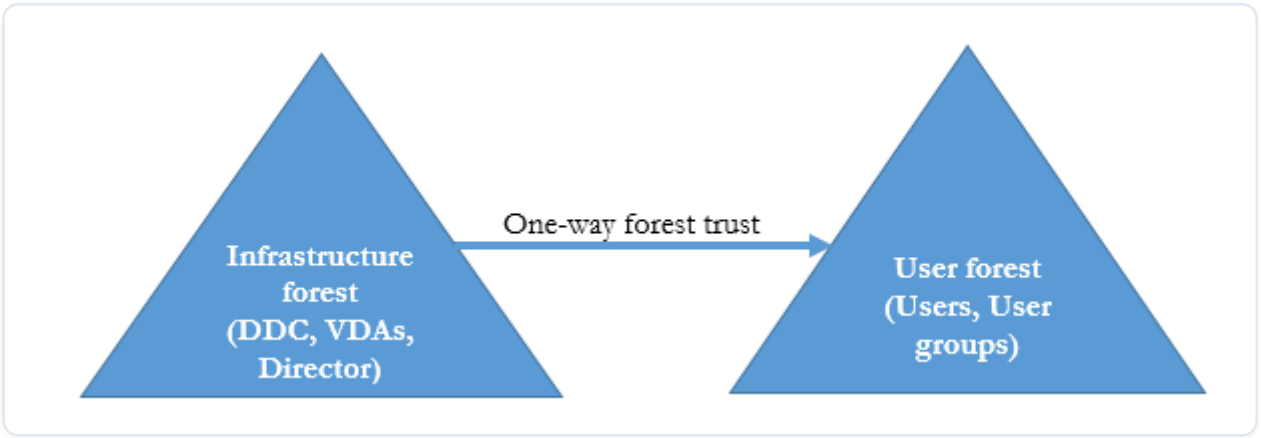
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

Para cada domínio na lista, o Director tenta realizar pesquisas no nível da floresta. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

### Configuração de grupo local de domínio

A maioria dos Provedores de Serviços Citrix (CSPs) possui configurações de ambiente semelhantes, consistindo em VDAs, DCs e Director na floresta de Infraestrutura. Os registros de usuários ou grupos de usuários pertencem à floresta do Cliente. Existe uma relação de confiança de saída unidirecional da floresta de Infraestrutura para a floresta do Cliente.

Os administradores de CSP geralmente criam um grupo local de domínio na floresta de Infraestrutura e adicionam os usuários ou grupos de usuários da floresta do Cliente a este grupo local de domínio.




O Director pode suportar uma configuração multi-floresta como esta e monitorar as sessões de usuários configurados usando grupos locais de domínio.

1. Adicione as seguintes configurações de Aplicativos ao site do Director no Gerenciador do IIS:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> são nomes das florestas nas quais o grupo local de domínio existe.

2. Atribua o grupo local de domínio aos grupos de entrega no Web Studio.
3. Reinicie o IIS e faça login no Director novamente para que as alterações entrem em vigor. Agora, o Director pode monitorar e exibir as sessões desses usuários.

### Adicionar sites ao Director

Se o Director já estiver instalado, configure-o para funcionar com vários sites. Para configurar, use o Console do Gerenciador do IIS em cada servidor do Director para atualizar a lista de endereços de servidor nas configurações do aplicativo.

Adicione um endereço de um Controller de cada site à seguinte configuração:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController e SiteBController são os endereços de Delivery Controllers de dois sites diferentes.

### Desabilitar a visibilidade de aplicativos em execução no Gerenciador de Atividades

Por padrão, o Gerenciador de Atividades no Director exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Essas informações são visualizadas por todos os administradores que têm acesso ao recurso Gerenciador de Atividades no Director. Para funções de Administrador Delegado, isso inclui Administrador Completo, Administrador de grupo de entrega e Administrador de Help Desk.

Para proteger a privacidade dos usuários e dos aplicativos que eles estão executando, você pode desabilitar a guia **Aplicativos** para listar os aplicativos em execução.

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

1. No VDA, modifique a chave do registro em `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`. Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, portanto, não são exibidas no Gerenciador de Atividades.
2. No servidor com o Director instalado, modifique a configuração que controla a visibilidade dos aplicativos em execução. Por padrão, o valor é "true", o que permite a visibilidade dos aplicativos em execução na guia Aplicativos. Altere o valor para "false", o que desabilita a

visibilidade. Esta opção afeta apenas o Gerenciador de Atividades no Director, não o VDA. Modifique o valor da seguinte configuração: UI.TaskManager.EnableApplications = false

**Importante:**

Para desabilitar a visualização de aplicativos em execução, faça ambas as alterações para garantir que os dados não sejam exibidos no Gerenciador de Atividades.

## Configurar autenticação de cartão inteligente PIV

Este artigo lista a configuração necessária no Servidor Director e no Active Directory para habilitar o recurso de autenticação de cartão inteligente.

**Nota:**

A autenticação de cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

### Configuração do servidor Director

Execute as seguintes etapas de configuração no servidor Director:

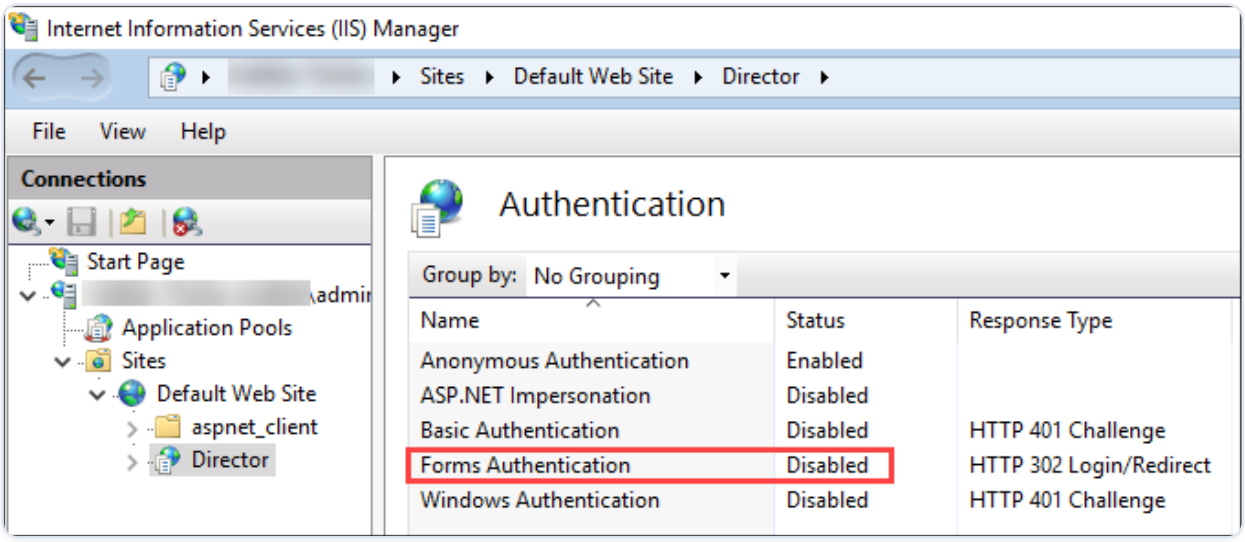
1. Instale e habilite a Autenticação de Mapeamento de Certificado de Cliente. Siga as instruções de **Autenticação de mapeamento de certificado de cliente usando o Active Directory** no documento da Microsoft, Autenticação de Mapeamento de Certificado de Cliente.
2. Desabilite a Autenticação de Formulários no site do Director.

   Inicie o Gerenciador do IIS.

   Vá para **Sites** \> **Default Web Site** \> **Director**.

   Selecione **Autenticação**.

   Clique com o botão direito em **Autenticação de Formulários** e selecione **Desabilitar.**



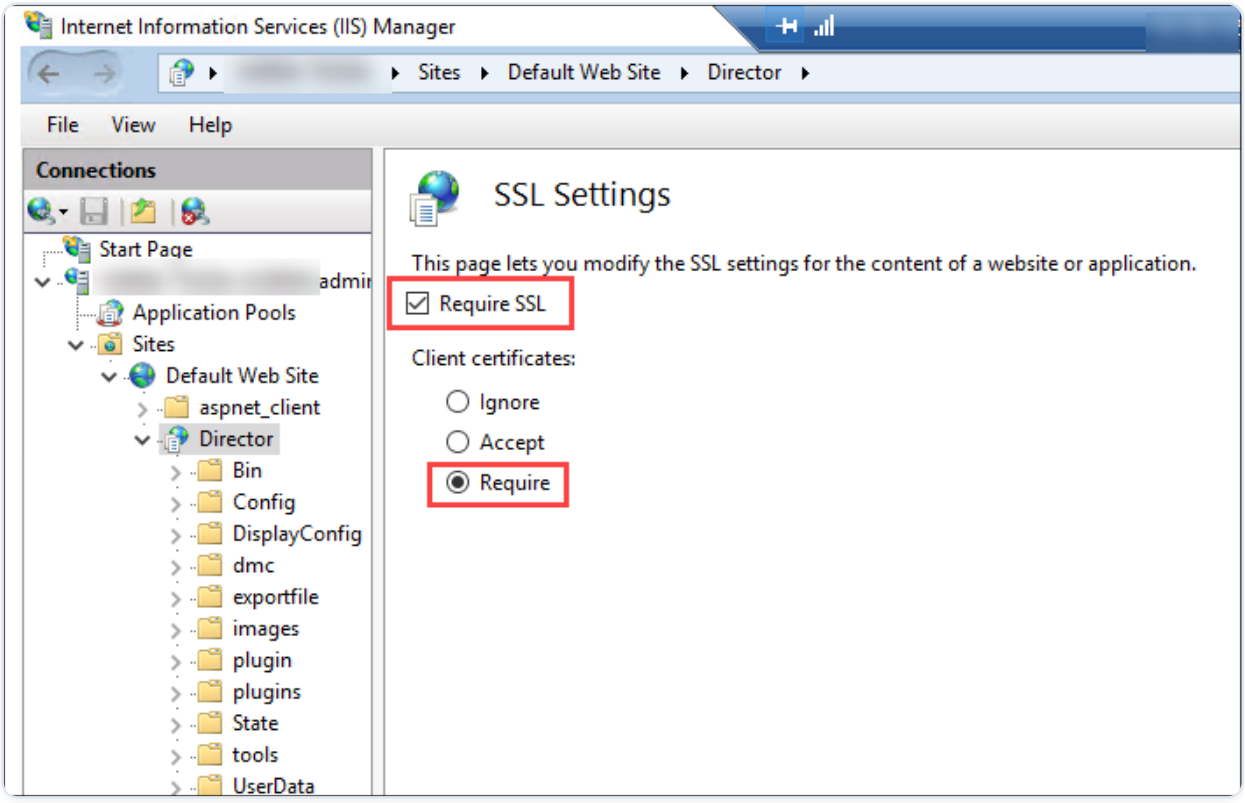

3. Configure a URL do Director para o protocolo https mais seguro (em vez de HTTP) para autenticação de certificado de cliente.

   a. Inicie o Gerenciador do IIS.

   b. Vá para **Sites** \> **Default Web Site** \> **Director**.

   c. Selecione **Configurações SSL.**

   d. Selecione **Exigir SSL** e **Certificados de cliente** \> **Exigir.**




4. Atualize o web.config. Abra o arquivo web.config (disponível em `c:\inetpub\wwwroot\Director`) usando um editor de texto.

Sob o elemento pai `<system.webServer>`, adicione o seguinte trecho como o primeiro elemento filho:

```
&lt;defaultDocument&gt;

   &lt;files&gt;

       &lt;add value="LogOn.aspx"/&gt;

   &lt;/files&gt;

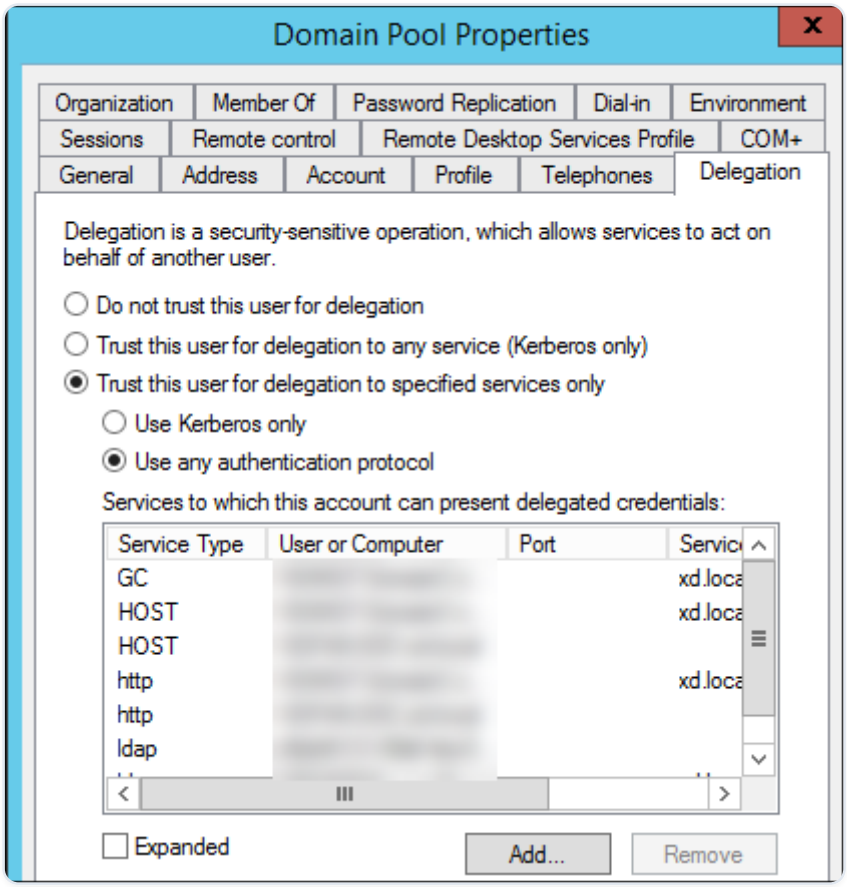
&lt;/defaultDocument&gt;
```

### Configuração do Active Directory

Por padrão, o aplicativo Director é executado com a propriedade de identidade do **Application Pool**. A autenticação por cartão inteligente requer delegação para a qual a identidade do aplicativo Director deve ter privilégios de Trusted Computing Base (TCB) no host de serviço.

A Citrix recomenda que você crie uma conta de serviço separada para a identidade do Pool de Aplicativos. Crie a conta de serviço e atribua privilégios TCB conforme as instruções no artigo da Microsoft MSDN, Protocol Transition with Constrained Delegation Technical Supplement.

Atribua a conta de serviço recém-criada ao pool de aplicativos do Director. A figura a seguir mostra a caixa de diálogo de propriedades de uma conta de serviço de exemplo, Domain Pool.

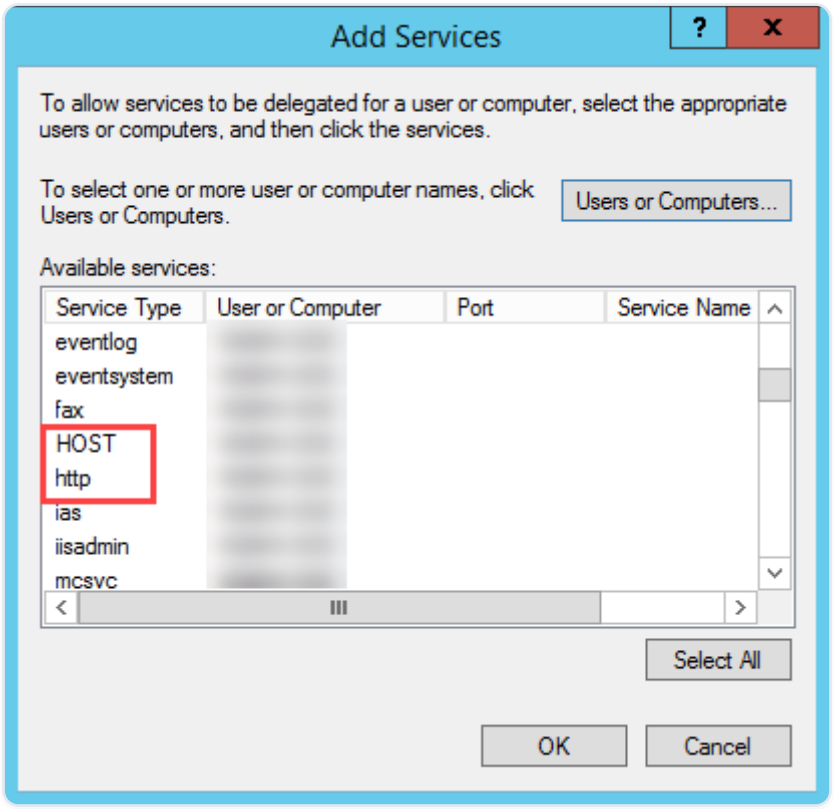



Configure os seguintes serviços para esta conta:

- Delivery Controller™: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

Para configurar,

1. Na caixa de diálogo de propriedades da conta de usuário, clique em **Adicionar.**
2. Na caixa de diálogo **Adicionar Serviços**, clique em Usuários ou Computadores.
3. Selecione o nome do host do Delivery Controller.
4. Na lista **Serviços disponíveis**, selecione HOST e **Tipo de Serviço** HTTP.




Da mesma forma, adicione Tipos de Serviço para os hosts do **Director** e do **Active Directory**.

### Criar registros de Nome Principal de Serviço

Você deve criar uma conta de serviço para cada servidor Director e IPs Virtuais (VIP) com balanceamento de carga usados para acessar um pool de servidores Director. Você deve criar registros de nome principal de serviço (SPN) para configurar uma delegação para a conta de serviço recém-criada.

- Use o seguinte comando para criar um registro SPN para um servidor Director:

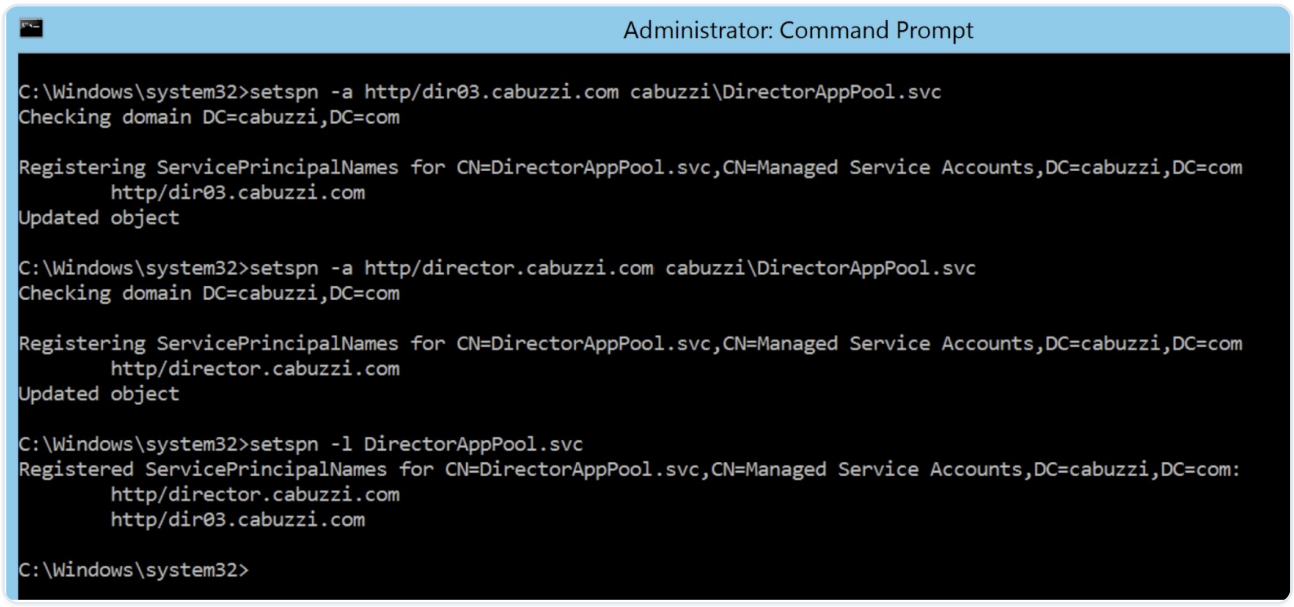
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- Use o seguinte comando para criar um registro SPN para um VIP com balanceamento de carga:

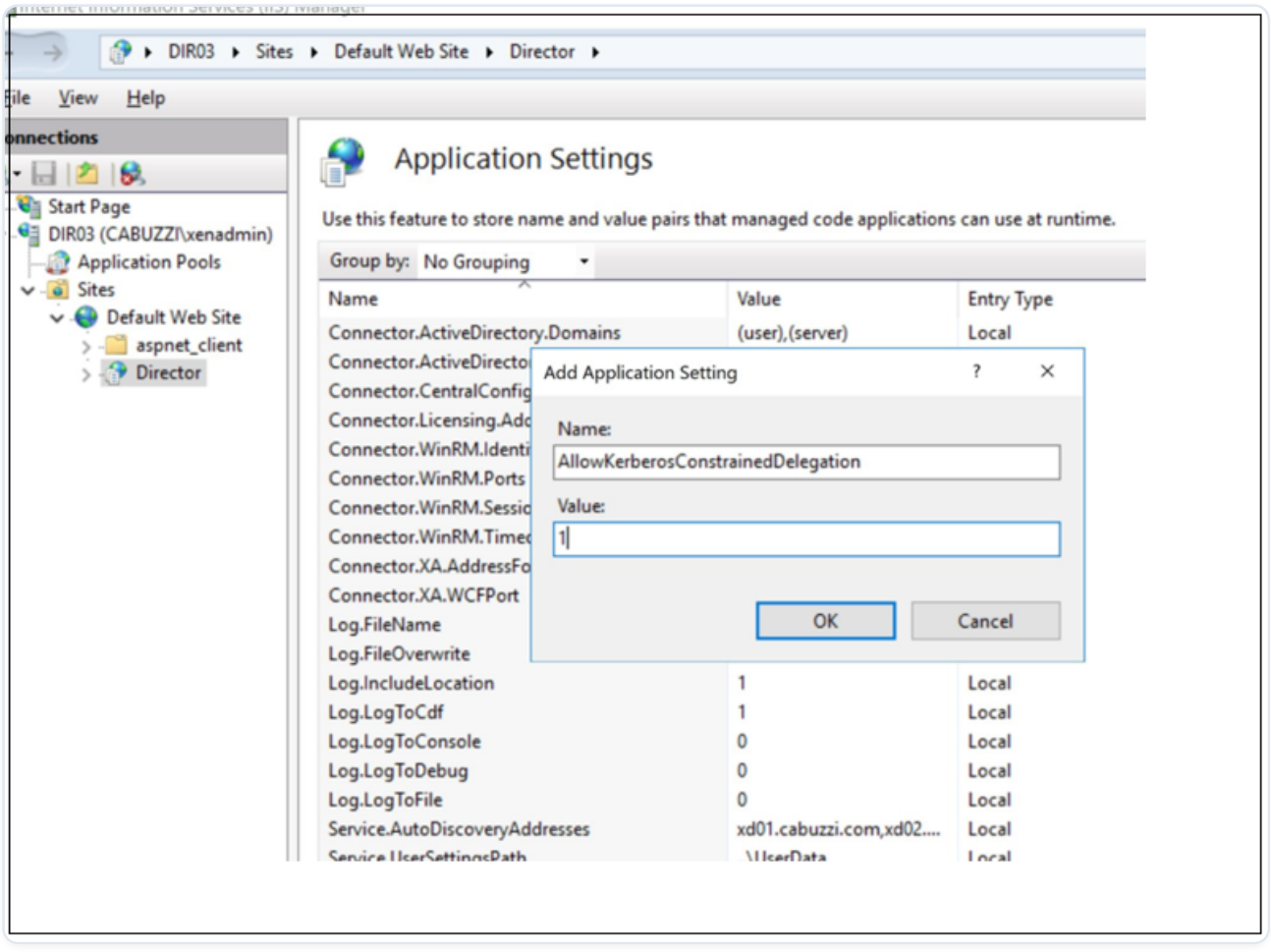
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- Use o seguinte comando para visualizar ou testar os SPNs criados:

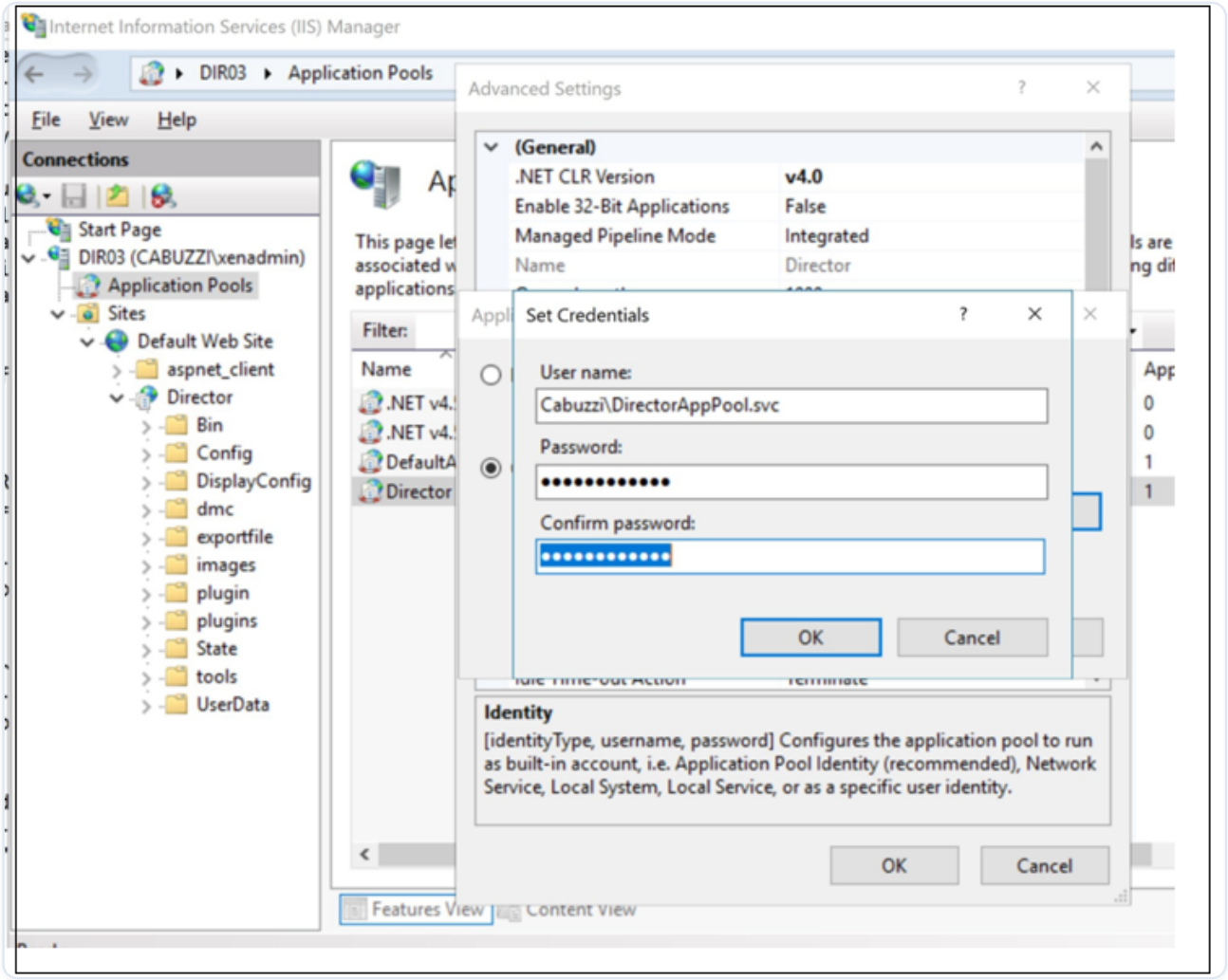
```
setspn –l <DirectorAppPoolServiceAcct>
```




- Selecione o diretório virtual do Director no painel esquerdo e clique duas vezes em **Application Settings**. Dentro da janela Application Settings, clique em **Adicionar** e certifique-se de que **AllowKerberosConstrainedDelegation** esteja definido como 1.



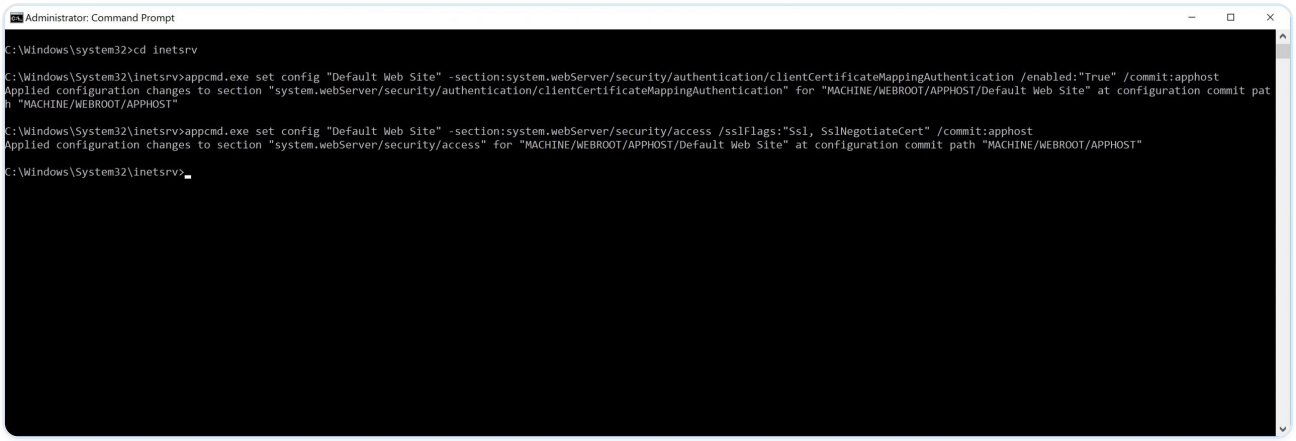
- Selecione **Application Pools** no painel esquerdo, clique com o botão direito do mouse no pool de aplicativos do Director e selecione **Advanced Settings**.
- Selecione **Identidade**, clique nas reticências (“…”) para inserir as credenciais de domínio\logon e senha da conta de serviço. Feche o console do IIS.




- Em um prompt de comando elevado, altere o diretório para C:\Windows\System32\inetsrv e insira os seguintes comandos:

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```




### Configuração do navegador Firefox

Para usar o navegador Firefox, instale o driver PIV disponível em OpenSC 0.17.0. Para obter instruções de instalação e configuração, consulte Installing OpenSC PKCS#11 Module in Firefox, Step by Step. Para obter informações sobre o uso do recurso de autenticação de cartão inteligente no Director, consulte a seção Use Director with PIV based smart card authentication no artigo do Director.

## Configurar análise de rede

> **Nota:** A disponibilidade deste recurso depende da licença da sua organização e das suas permissões de administrador.

> O Director se integra ao Citrix ADM para fornecer análise de rede e gerenciamento de desempenho:

- A análise de rede usa relatórios HDX™ Insight do Citrix ADM para fornecer uma visão contextual da rede para aplicativos e desktops. Com esse recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação.
- O gerenciamento de desempenho oferece retenção histórica e relatórios de tendências. Com a retenção histórica de dados em vez da avaliação em tempo real, você pode criar relatórios de tendências, incluindo tendências de capacidade e integridade.

Depois de habilitar esse recurso no Director, os relatórios do HDX Insight fornecem ao Director informações adicionais:

- A guia Rede na página Tendências mostra os efeitos de latência e largura de banda para aplicativos, desktops e usuários em toda a sua implantação.
- A página Detalhes do Usuário mostra informações de latência e largura de banda específicas para uma sessão de usuário em particular.

**Limitações:**

- Na exibição Tendências, os dados de logon da conexão HDX não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.

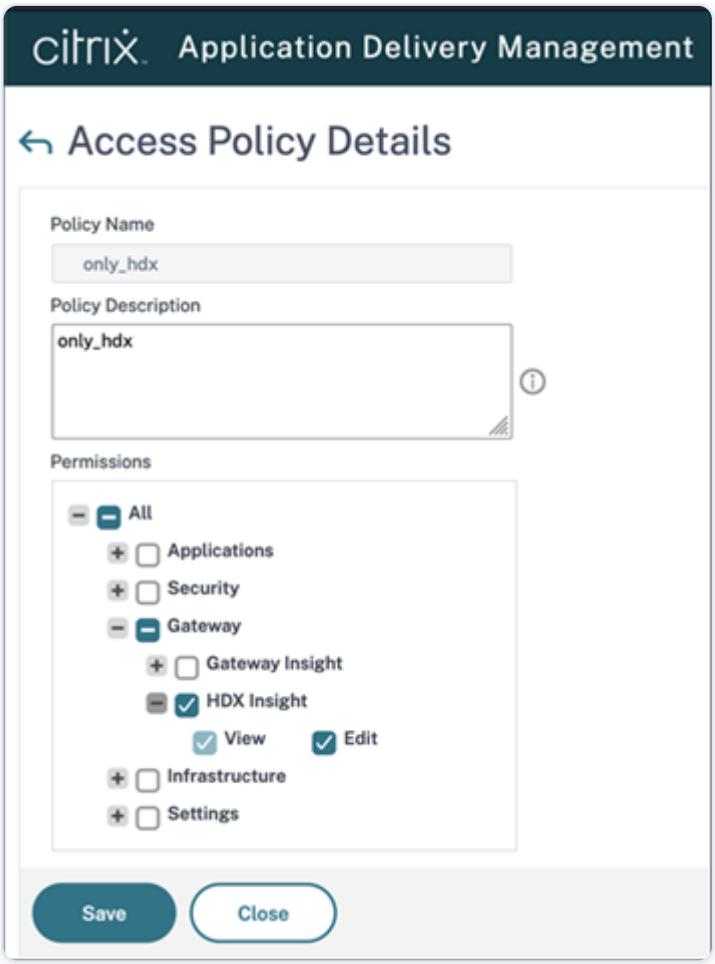
Para habilitar a análise de rede, você deve instalar e configurar o Citrix ADM no Director. O Director requer o Citrix ADM Versão 11.1 Build 49.16 ou posterior. O MAS é um dispositivo virtual que é executado no XenServer. Usando a análise de rede, o Director se comunica e coleta as informações relacionadas à sua implantação.

Para obter mais informações, consulte a documentação do Citrix ADM.

> **Nota:**
>
> O Citrix NetScaler Insight Center atingiu sua data de Fim de Manutenção em 15 May 2018. Consulte a Matriz de Produtos Citrix. Integre o Director ao Citrix ADM para análise de rede. Para migrar seu NetScaler Insight Center para o Citrix ADM, consulte Migrar do NetScaler Insight Center para o Citrix ADM.

1. No servidor onde o Director está instalado, localize a ferramenta de linha de comando DirectorConfig em `C:\inetpub\wwwroot\Director\tools` e execute-a com o parâmetro /configNetscaler a partir de um prompt de comando.
2. Quando solicitado, insira o nome da máquina Citrix ADM (FQDN ou endereço IP), o nome de usuário, a senha, o tipo de conexão HTTPS (preferencial em relação ao HTTP) e escolha a integração do Citrix ADM.
3. Para verificar as alterações, faça logoff e faça login novamente.

> **Nota:**
>
> Por motivos de segurança, é recomendado criar uma função personalizada para a integração do ADM com o Director com permissão suficiente para acessar apenas o HDX Insight.




Para obter mais informações, consulte Configurar políticas de acesso.

## Administração delegada e Director

A administração delegada usa três conceitos: administradores, funções e escopos. As permissões são baseadas na função de um administrador e no escopo dessa função. Por exemplo, um administrador pode receber uma função de administrador de Help Desk onde o escopo envolve a responsabilidade por usuários finais em apenas um site.

Para obter informações sobre a criação de administradores delegados, consulte o artigo principal sobre administração delegada.

As permissões administrativas determinam a interface do Director apresentada aos administradores e as tarefas que eles podem realizar. As permissões determinam:

- As exibições que o administrador pode acessar, coletivamente referidas como uma exibição.
- Os desktops, máquinas e sessões que o administrador pode visualizar e interagir.
- Os comandos que o administrador pode executar, como sombrear a sessão de um usuário ou habilitar o modo de manutenção.

As funções e permissões integradas também determinam como os administradores usam o Director:

| FUNÇÃO DE ADMINISTRADOR | PERMISSÕES NO DIRECTOR |
|---|---|
| Administrador Completo | Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o modo de manutenção e exportar dados de tendências. |
| Administrador de grupo de entrega | Acesso total a todas as visualizações e pode executar todos os comandos, incluindo o espelhamento da sessão de um usuário, gerenciamento de energia e gerenciamento de sessão, habilitação do modo de manutenção e exportação de dados de tendências. |
| Administrador Somente Leitura | Pode acessar todas as visualizações e ver todos os objetos em escopos especificados e informações globais. Pode baixar relatórios de canais HDX™ e pode exportar dados de Tendências usando a opção Exportar na visualização Tendências. Não pode executar nenhum outro comando ou alterar nada nas visualizações. |
| Administrador de Help Desk | Pode acessar apenas as visualizações de Help Desk e Detalhes do Usuário e pode visualizar apenas objetos que o administrador está delegado a gerenciar. Pode espelhar a sessão de um usuário e executar comandos para esse usuário. Pode realizar operações de modo de manutenção. Pode usar opções de controle de energia para Máquinas OS de sessão única. Não pode acessar as visualizações de Painel, Tendências, Alertas ou Filtros. Não pode usar opções de controle de energia para máquinas OS de múltiplas sessões. |
| Administrador de catálogo de máquinas | Pode acessar apenas a página Detalhes da Máquina (pesquisa baseada em máquina). |

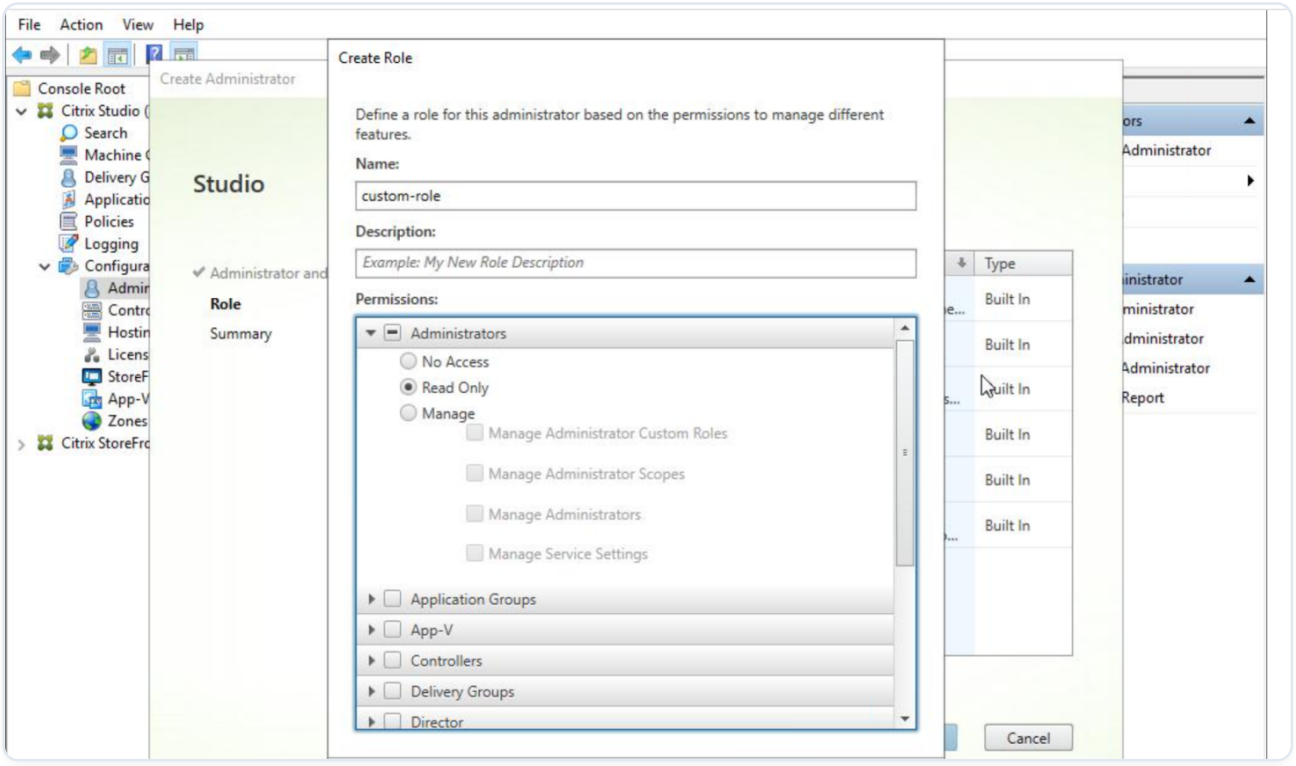
| FUNÇÃO DE ADMINISTRADOR | PERMISSÕES NO DIRECTOR |
| --- | --- |
| Administrador de Host | Sem acesso. Este administrador não é suportado para o Director e não pode visualizar dados. |

### Configurar funções personalizadas para administradores do Director

No Studio, você também pode configurar funções personalizadas específicas do Director para corresponder mais de perto aos requisitos da sua organização e delegar permissões de forma mais flexível. Por exemplo, você pode restringir a função de administrador de Help Desk integrada para que este administrador não possa desconectar sessões.

Se você criar uma função personalizada com permissões do Director, também deverá conceder a essa função outras permissões genéricas:

- Permissão de Delivery Controller™ para fazer logon no Director - pelo menos acesso somente leitura no nó Administrador
- Permissões para grupos de entrega para visualizar os dados relacionados a esses grupos de entrega no Director - pelo menos acesso somente leitura

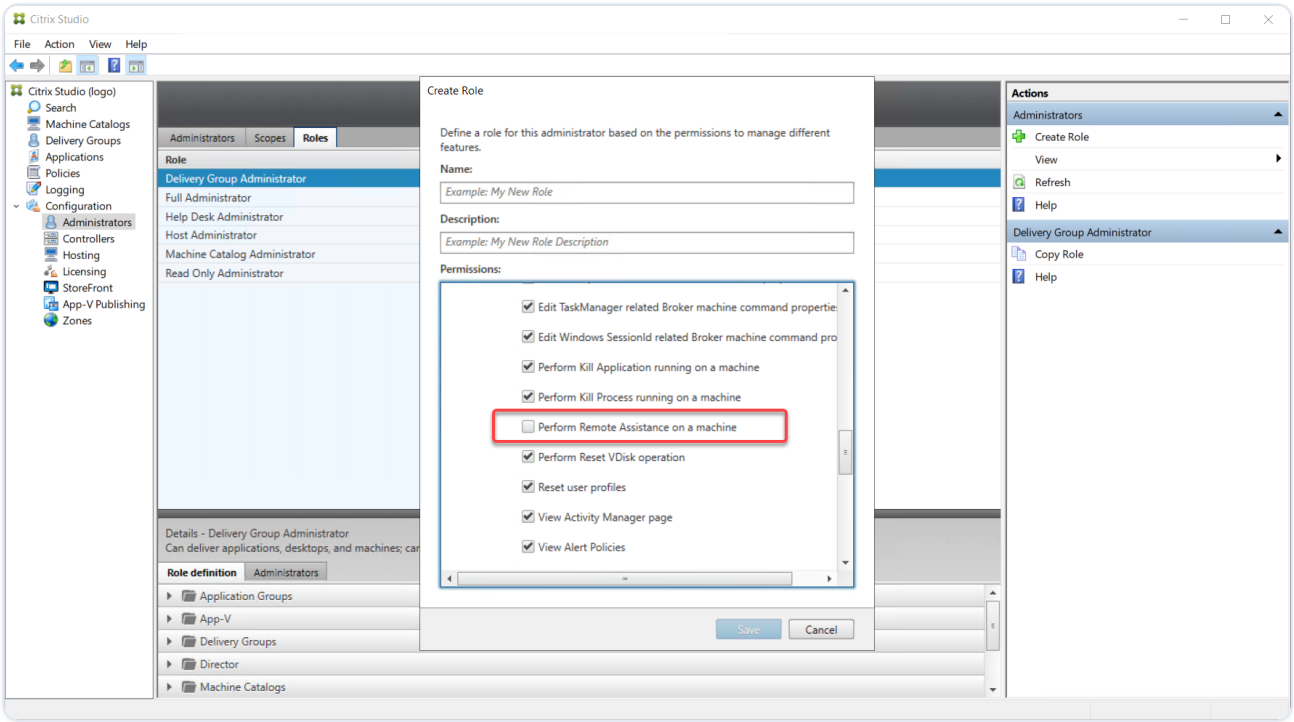



Como alternativa, você pode criar uma função personalizada copiando uma função existente e incluindo permissões extras para diferentes exibições. Por exemplo, você pode copiar a função de Help Desk e incluir permissões para exibir as páginas Painel ou Filtros.

Selecione as permissões do Director para a função personalizada, que incluem:

- Executar Encerrar Aplicativo em execução em uma máquina
- Executar Encerrar Processo em execução em uma máquina
- Executar Assistência Remota em uma máquina
- Redefinir perfis de usuário
- Exibir página Detalhes do Cliente
- Visualizar página do Painel
- Exibir página Filtros
- Exibir página Detalhes da Máquina
- Visualizar página de Tendências
- Exibir página Detalhes do Usuário

Neste exemplo, o Sombreamento (Executar Assistência Remota em uma máquina) está desativado.




Uma permissão pode ter dependências de outras permissões para se tornar aplicável na interface do usuário. Por exemplo, selecionar a permissão **Executar Encerrar Aplicativo em execução em uma máquina** habilita a funcionalidade **Encerrar Aplicativo** apenas nos painéis para os quais a função tem permissão. Você pode selecionar as seguintes permissões de painel:

- Exibir página Filtros
- Visualizar página de Detalhes do Usuário

- Visualizar página de Detalhes da Máquina
- Visualizar página de Detalhes do Cliente

Além disso, da lista de permissões para outros componentes, considere estas permissões de grupos de entrega:

- Ativar/desativar o modo de manutenção de uma máquina usando a associação a grupos de entrega.
- Executar operações de energia em máquinas Windows Desktop usando a associação a grupos de entrega.
- Executar gerenciamento de sessão em máquinas usando a associação a grupos de entrega.

## Implantação segura do Director

Este artigo destaca áreas que podem ter um impacto na segurança do sistema ao implantar e configurar o Director.

### Configurar o Microsoft Internet Information Services (IIS)

Você pode configurar o Director com uma configuração restrita do IIS.

#### Limites de reciclagem do Pool de Aplicativos

Você pode definir os seguintes limites de reciclagem do Pool de Aplicativos:

- Limite de Memória Virtual: 4.294.967.295
- Limite de Memória Privada: O tamanho da memória física do servidor StoreFront™
- Limite de Solicitações: 4.000.000.000

#### Extensões de nome de arquivo

Você pode não permitir 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

- .GIF
- .JSON
- .WOFF
- .woff2
- .TTF

O Director requer os seguintes verbos HTTP na Filtragem de Solicitações. Você pode desabilitar verbos não listados.

- GET
- POST
- HEAD

O Director não requer:

- Filtros ISAPI
- Extensões ISAPI
- Programas CGI
- Programas FastCGI

> **Importante:**
>
> - O Director requer Confiança Total. Não defina o nível de confiança global do .NET como Alto ou inferior.
> - O Director mantém um pool de aplicativos separado. Para modificar as configurações do Director, selecione o site do Director e modifique.

### Configurar direitos de usuário

Quando o Director é instalado, seus pools de aplicativos recebem o seguinte:

- Direito de logon de **Fazer logon como um serviço**
- Privilégios de **Ajustar cotas de memória para um processo**, **Gerar auditorias de segurança** e **Substituir um token de nível de processo**

Os direitos e privilégios mencionados são comportamentos normais de instalação quando os pools de aplicativos são criados.

Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Director e são desativados automaticamente.

### Comunicações do Director

Em um ambiente de produção, use os protocolos de segurança do Protocolo de Internet (IPsec) ou HTTPS para proteger os dados que transitam entre o Director e seus servidores.

O IPsec é um conjunto de extensões padrão para o Protocolo de Internet que fornece comunicações autenticadas e criptografadas com integridade de dados e proteção contra repetição. Como o IPsec é um conjunto de protocolos de camada de rede, protocolos de nível superior podem usá-lo sem modificação. O HTTPS usa os protocolos Transport Layer Security (TLS) para fornecer criptografia de dados forte.

**Nota:**

- A Citrix® recomenda fortemente que você restrinja o acesso ao console do Director dentro da rede intranet.
- A Citrix recomenda fortemente que você não habilite conexões não seguras ao Director em um ambiente de produção.
- As comunicações seguras do Director exigem configuração para cada conexão separadamente.
- O protocolo SSL não é recomendado. Use o protocolo TLS mais seguro em vez disso.
- Proteja suas comunicações com o Citrix ADC usando TLS, não IPsec.

Para proteger as comunicações entre o Director e os servidores Citrix Virtual Apps and Desktops (para monitoramento e relatórios), consulte Segurança de Acesso a Dados.

Para proteger as comunicações entre o Director e o Citrix ADC (para Citrix Insight), consulte Configurar análise de rede.

Para proteger as comunicações entre o Director e o servidor de licenças, consulte Proteger o Console de Administração de Licenças.

### Separação de segurança do Director

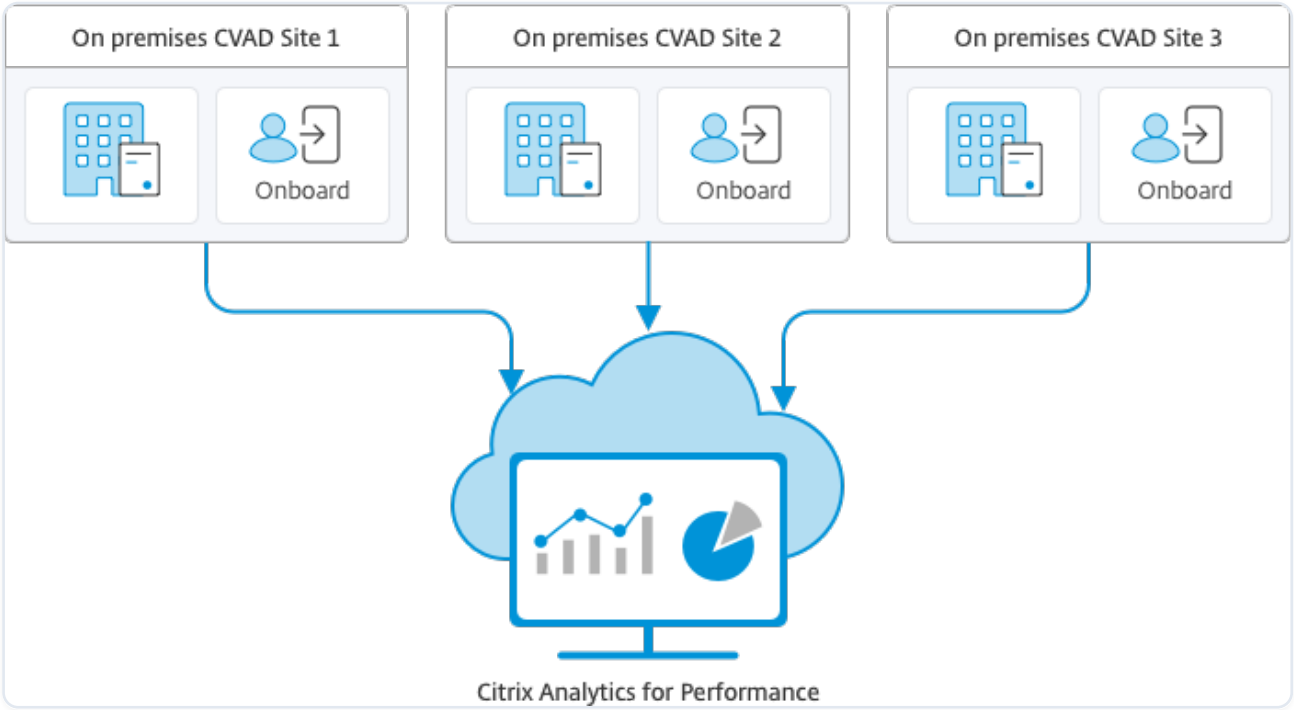
Você pode implantar quaisquer aplicativos web no mesmo domínio web (nome de domínio e porta) que o Director. No entanto, quaisquer riscos de segurança nesses aplicativos web podem potencialmente reduzir a segurança da sua implantação do Director. Onde um maior grau de separação de segurança é necessário, a Citrix recomenda que você implante o Director em um domínio web separado.

## Configurando sites locais com Citrix Analytics for Performance™

O Citrix Analytics for Performance (Performance Analytics) é a solução abrangente de monitoramento de desempenho do Serviço de Nuvem Citrix Analytics. O Performance Analytics fornece insights e análises avançadas construídas sobre métricas de desempenho. O Performance Analytics ajuda você a monitorar e visualizar as métricas de uso e desempenho de um ou mais sites do Citrix Virtual Apps and Desktops™ em sua organização.

Para obter mais informações sobre o Performance Analytics, consulte o artigo do Performance Analytics.

Você pode enviar dados de desempenho do seu site para o Citrix Analytics for Performance no Citrix Cloud™ para aproveitar seus recursos avançados de análise de desempenho. Para visualizar e usar o Performance Analytics, você deve primeiro configurar seus sites locais com o Citrix Analytics for Performance na guia **Analytics** no **Director**.




O Performance Analytics acessa os dados de forma segura e nenhum dado é transferido do Citrix Cloud para o ambiente local.

### Pré-requisitos

Para configurar o Citrix Analytics for Performance a partir do Director, nenhum novo componente precisa ser instalado. Certifique-se de que os seguintes requisitos sejam atendidos:

- Seu Delivery Controller e Director estão na versão 1912 CU2 ou posterior. Para obter mais informações, consulte Matriz de compatibilidade de recursos.

> **Nota:**
>
> - A configuração do seu site local com o Citrix Analytics for Performance a partir do Director pode falhar se o Delivery Controller estiver executando uma versão do Microsoft .NET Framework anterior à 4.8. Como solução alternativa, atualize o .NET Framework em seu Delivery Controller para a versão 4.8. LCM-9255.
> - Ao configurar seu site local executando o Citrix Virtual Apps and Desktops versão 2012 com o Citrix Analytics for Performance a partir do Director, a configuração pode falhar após algumas horas ou após uma reinicialização do Serviço de Monitoramento Citrix no Delivery Controller. A guia Analytics exibe um status Não Conectado neste caso. Como solução alternativa, crie uma pasta Encryption no registro no Delivery Controller, Local: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor, Nome da Pasta: Encryption. Certifique-se de que a conta CitrixMonitor tenha Acesso de Controle Total na pasta Encryption. Reinicie o Serviço de Monitoramento Citrix.DIR-14324.

- O acesso à guia **Analytics** para realizar esta configuração está disponível apenas para administradores completos.
- Para que o Performance Analytics acesse as métricas de desempenho, o acesso à internet de saída está disponível em todos os Delivery Controllers e nas máquinas onde o Director está instalado. Especificamente, garanta a acessibilidade aos seguintes URLs:
  - Registro de Chave Citrix: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Caso os Delivery Controllers e as máquinas do Director estejam em uma intranet e o acesso à internet de saída seja feito por um servidor proxy, certifique-se do seguinte:
- O servidor proxy deve permitir a lista de URLs anterior.

- Adicione a seguinte configuração nos arquivos Director web.config e citrix.monitor.exe.config. Certifique-se de adicionar esta configuração dentro das tags **configuration**:

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - O Director web.config está localizado em `C:\inetpub\wwwroot\Director\web.config` na máquina onde o Director está instalado.
  - O citrix.monitor.exe.config está localizado em `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` na máquina onde o Delivery Controller está instalado.

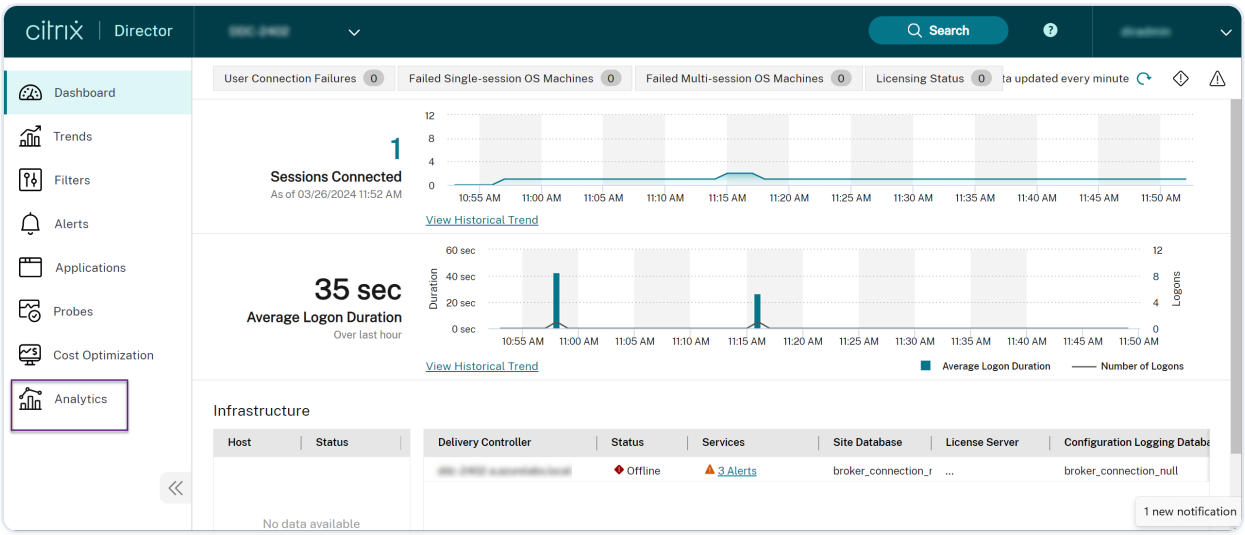
  Essa configuração é fornecida pela Microsoft no IIS. Para obter mais informações, consulte `https://docs.microsoft.com/pt-br/dotnet/framework/network-programming/proxy-configuration`. O campo **defaultproxy** no arquivo de configuração controla o acesso de saída do Director e do Monitor Service. A configuração e a comunicação com o Performance Analytics exigem que o campo **defaultproxy** seja definido como **true**. É possível que as políticas em vigor definam este campo como false. Nesse caso, você deve definir manualmente o campo como true. Faça um backup dos arquivos de configuração antes de fazer as alterações. Reinicie o serviço de Monitoramento no Delivery Controller™ para que as alterações sejam aplicadas.

- Você tem um direito ativo do Citrix Cloud para o Citrix Analytics for Performance.
- Sua conta do Citrix Cloud é uma conta de Administrador com direitos à Experiência de Registro de Produto. Para obter mais informações sobre permissões de administrador, consulte Modificar Permissões de Administrador.

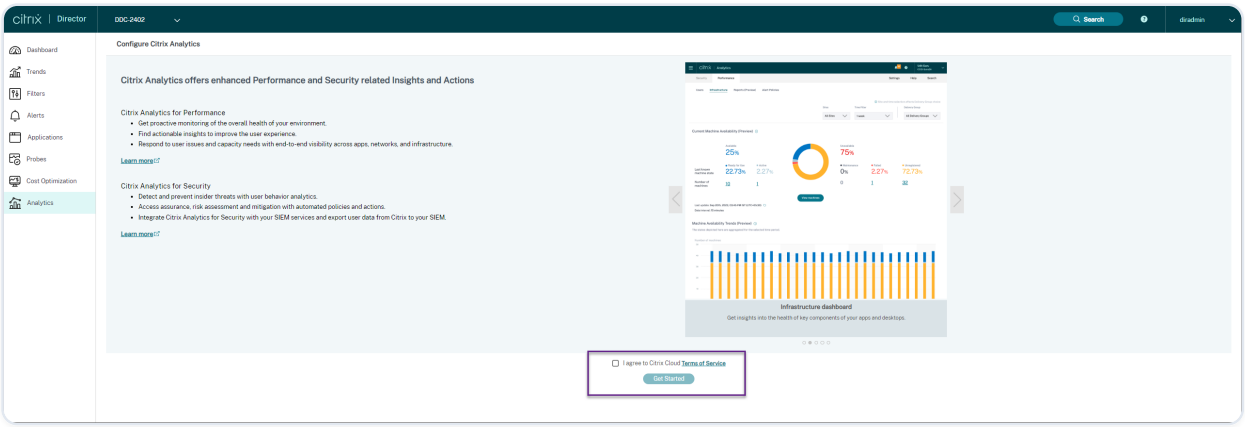
### Etapas de configuração

Depois de verificar os pré-requisitos, faça o seguinte:

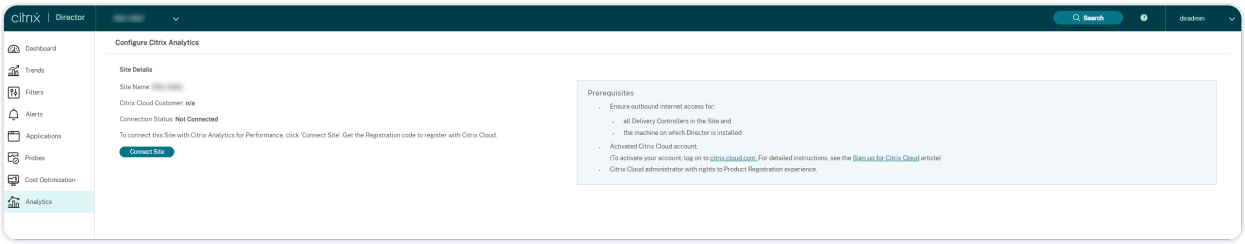
1. Faça login no Director como administrador completo e selecione o site que você deseja configurar com o Performance Analytics. A página do Painel do Director é exibida.




2. Clique na guia **Analytics**. A página **Configurar Citrix Analytics** é exibida.

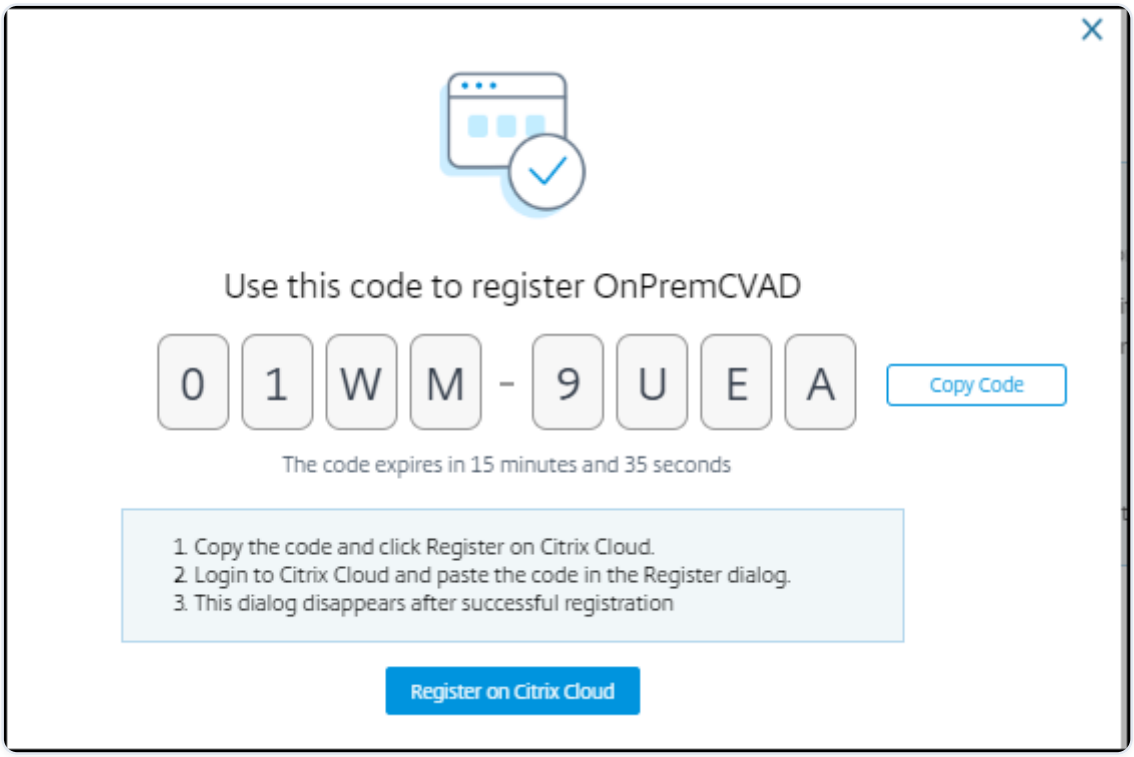



3. Revise as etapas, selecione os termos de serviço e clique em **Começar**. A página **Detalhes do Site** é exibida.

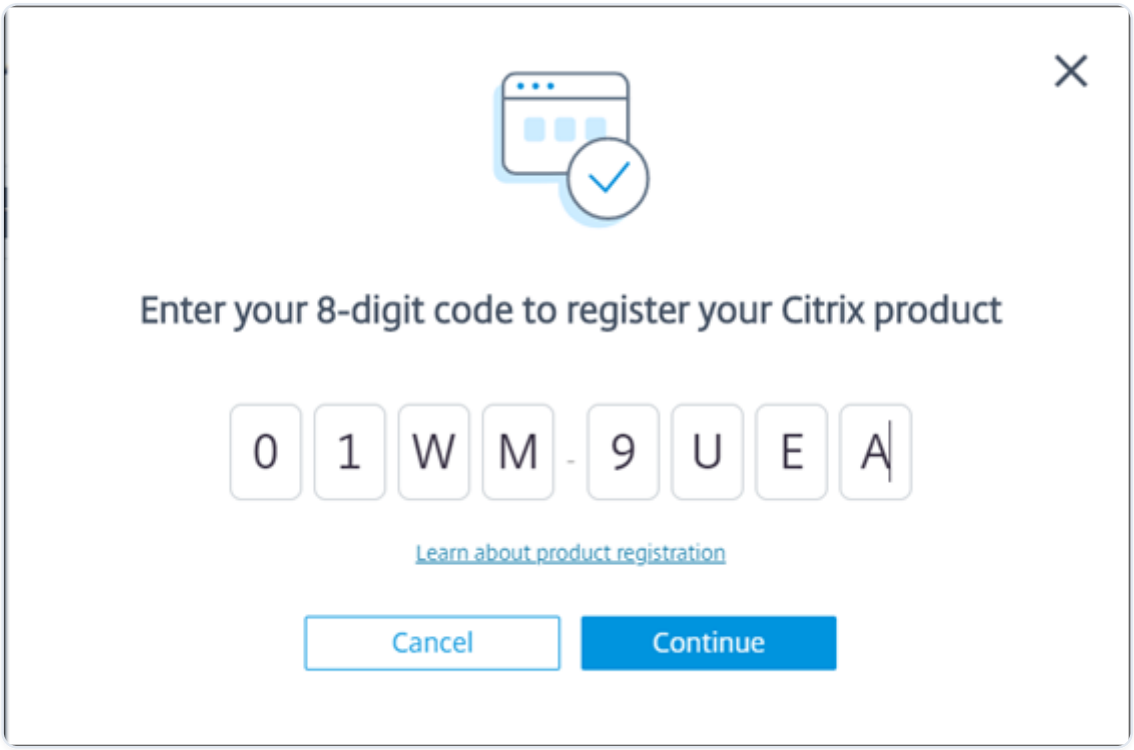



4. Revise os pré-requisitos e certifique-se de que foram atendidos. Revise os detalhes do site.
5. Clique em **Conectar Site** para iniciar o processo de configuração.

   Um código de registro exclusivo de 8 dígitos é gerado para ser usado para registrar este site no Citrix Cloud.

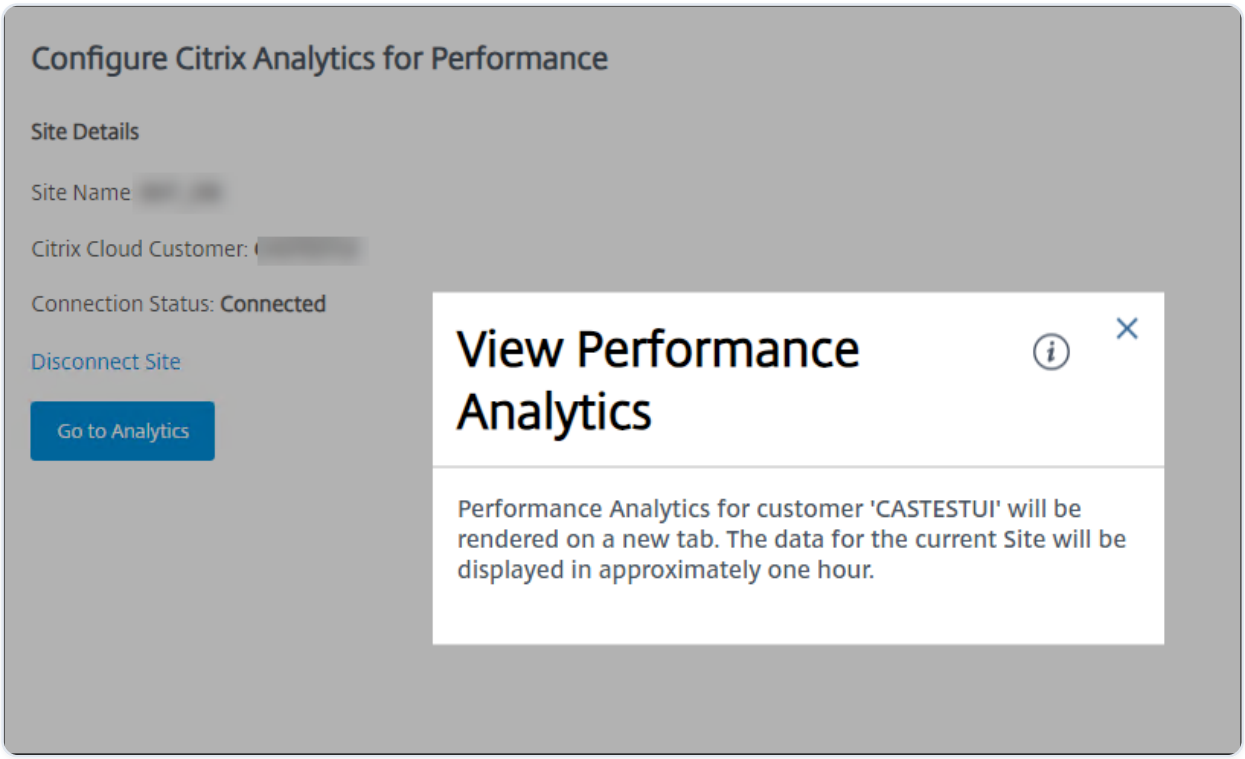



6. Clique em **Copiar Código** para copiar o código e, em seguida, clique em **Registrar no Citrix Cloud**. Você será redirecionado para o URL de registro no Citrix Cloud.
7. Faça login com suas credenciais do Citrix Cloud e selecione seu cliente.
8. Cole o código de registro copiado na página Registros de Produto no Citrix Cloud. Clique em **Continuar** para registrar. Revise os detalhes do registro e clique em **Registrar**.

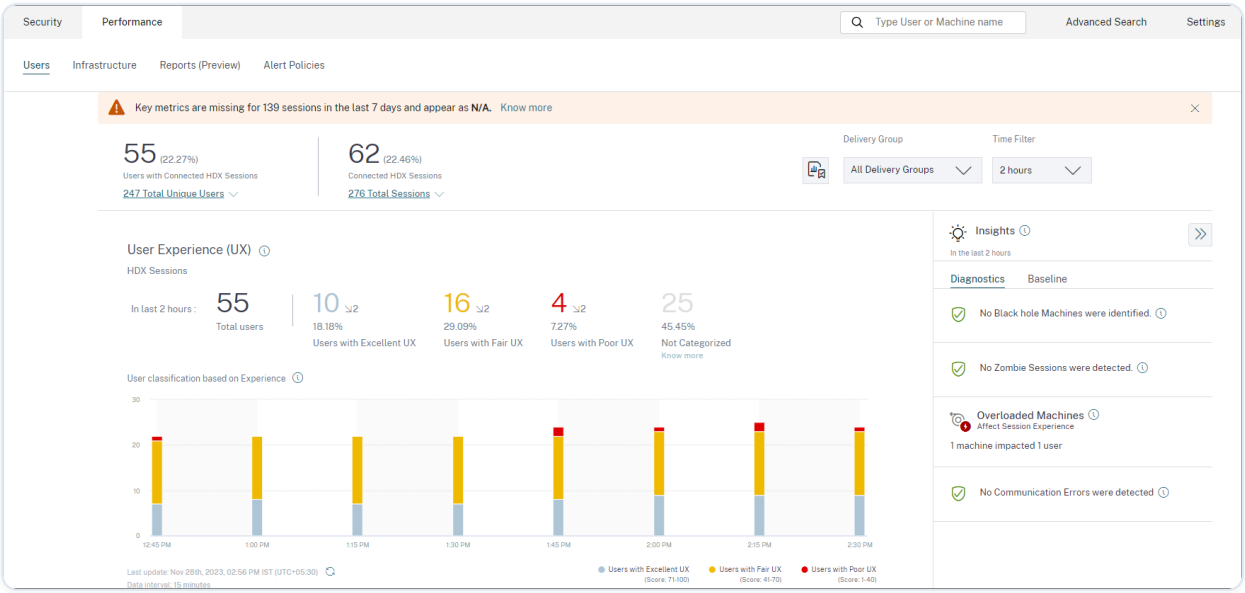



Seu site local se registra no Citrix Cloud.

9. No **Director**, clique em **Ir para Análise** na guia **Análise**.




O Performance Analytics é aberto em uma nova guia no seu navegador.




Se sua sessão do Citrix Cloud tiver expirado, você poderá ser redirecionado para a página de logon da conta Citrix.com ou My Citrix.

10. Para registrar vários sites no Performance Analytics, repita as etapas de configuração anteriores para cada site a partir do Director. As métricas para todos os sites configurados são exibidas no painel do Performance Analytics.

    Caso você tenha mais de uma instância do Director em execução por site, configure a partir de qualquer instância do Director. Todas as outras instâncias do Director conectadas ao site são atualizadas na próxima atualização após o processo de configuração.

11. Para desconectar seu site do Citrix Cloud, clique em **Desconectar Site**. Esta opção exclui a configuração existente.

> **Notas:**
>
> Na primeira vez que você configura um site, os eventos do site podem levar algum tempo (aproximadamente uma hora) para serem processados; causando um atraso na exibição das métricas no painel do Performance Analytics. Depois disso, os eventos são atualizados em intervalos regulares.
>
> Após a desconexão, a transmissão de dados da conta antiga continua por algum tempo até que os eventos da nova conta sejam transmitidos. Por aproximadamente uma hora após a interrupção da transmissão de dados, as análises relacionadas à conta antiga permanecem exibidas no Painel do Performance Analytics.
>
> Após a expiração do direito ao serviço Citrix Analytics, leva até um dia para parar de enviar as métricas do site para o Performance Analytics.

## Lançamento independente do Director para implantações LTSR

O lançamento independente do Director para implantações LTSR agora oferece uma opção para acessar os recursos mais recentes do Director para solução de problemas e monitoramento aprimorados em ambientes Citrix® para ambientes LTSR compatíveis. Esse recurso permite que você use a versão mais recente do Director em suas implantações 2402 LTSR. Além disso, fornece acesso a recursos lançados após o anúncio do LTSR sem impactar a infraestrutura de entrega de aplicativos.

Para obter informações sobre os recursos do Director que fazem parte das versões atuais após o lançamento do 2402 LTSR, consulte o seguinte:

- Lançamento do Citrix Virtual Apps and Desktops 2407
- Lançamento do Citrix Virtual Apps and Desktops 2411

Para saber mais sobre recursos específicos do Director com a versão mínima do VDA, consulte Matriz de Versões do Director.

### Benefícios

- **Acesso a novos recursos**: Obtenha acesso aos recursos do Director lançados após o anúncio do LTSR 2402, incluindo aqueles nas versões cumulativas (CR) do Citrix Virtual Apps and Desktops™ 2407 e 2411.
- **Atualizações direcionadas:** Atualize apenas o componente do serviço Director e Monitoramento sem impactar o restante da sua infraestrutura LTSR.
- **Compatibilidade LTSR**: Mantenha seu ambiente LTSR enquanto se beneficia das mais recentes melhorias do Director.
- **Opção de reversão:** Você tem a flexibilidade de reverter para a versão anterior do Director, se necessário.

### Consideração principal

O componente Director atualizado é compatível com LTSR, mas não é coberto pelo suporte de componentes principais do LTSR. No entanto, o restante da sua infraestrutura LTSR mantém seu suporte existente.

### Pré-requisitos

- Certifique-se de estar usando um site Citrix Virtual Apps and Desktops 2402 LTSR CU1.
- Certifique-se de que está a utilizar o Microsoft SQL Server versão 2019 ou posterior.

### Visão geral de alto nível

Para atualizar um site do Citrix Virtual Apps and Desktops 2402 LTSR CU1 com os recursos mais recentes da Versão Atual, siga estes passos:

1. **Faça backup do seu banco de dados**: Antes de atualizar, certifique-se de fazer backup do banco de dados de Monitoramento. Este procedimento é crucial, pois o processo de atualização também atualiza o banco de dados.
2. **Atualize seu site**: Prossiga com a atualização do seu site para incorporar os novos recursos da versão atual.
3. **Opção de reversão**: Se você decidir não continuar com o site atualizado, poderá reverter para o seu site anterior usando as etapas de reversão.

### Etapas de atualização

1. Faça um backup do banco de dados do serviço Monitor.
2. Clique em **Atualizar** no instalador do Citrix Virtual Apps and Desktops.

3. Aceite o contrato de licença.
4. Na tela **Componentes Principais**, selecione uma das seguintes opções:
   - **Delivery Controller™** - Se esta opção for selecionada sozinha, apenas o Serviço Monitor da Versão Atual será instalado.
   - **Director** - Se esta opção for selecionada sozinha, apenas o Serviço Director da Versão Atual será instalado.
   - **Delivery Controller** e **Director** - Se ambas as opções forem selecionadas, a Versão Atual do Director e do Serviço Monitor serão instaladas.
5. Na tela **Recursos**, selecione a caixa de seleção **Instalar Director Current Release** `<version>`.

   > **Observação:**
   >
   > A caixa de seleção **Instalar Director Current Release** `<version>` está disponível para seleção somente se uma das opções na 4ª etapa for selecionada.

6. Siga as instruções na tela para concluir a atualização.
7. Na página **Resumo**, você pode revisar os componentes que serão instalados. Com base na seleção na página **Componentes Principais** e na página **Recursos**, a instalação do componente é a seguinte:

| SELEÇÃO DA PÁGINA COMPONENTES PRINCIPAIS | SELEÇÃO DA CAIXA DE SELEÇÃO INSTALAR DIRECTOR CURRENT RELEASE `<VERSION>` | INSTALAÇÃO DO COMPONENTE |
|---|---|---|
| Delivery Controller | Selecionado | A versão atual do Serviço de Monitoramento é instalada. |
| Delivery Controller | Não selecionado | A Atualização Cumulativa do Serviço de Monitoramento é instalada. |
| Director | Selecionado | A versão atual do Serviço Director é instalada. |

| SELEÇÃO DA PÁGINA COMPONENTES PRINCIPAIS | SELEÇÃO DA CAIXA DE SELEÇÃO INSTALAR DIRECTOR CURRENT RELEASE `<VERSION>` | INSTALAÇÃO DO COMPONENTE |
|---|---|---|
| Director | Não selecionado | A Atualização Cumulativa do Serviço Director é instalada. |
| Delivery Controller e Director | Selecionado | A versão atual do Serviço de Monitoramento e do Serviço do Director estão instaladas. |
| Delivery Controller e Director | Não selecionado | A Atualização Cumulativa do Serviço de Monitoramento e do Serviço do Director estão instaladas. |

8. Assim que a instalação for concluída, selecione a caixa de seleção **Abrir Citrix Site Manager**.
9. Inicie a atualização automática do site.
10. Verifique se os novos recursos estão disponíveis no Director.

#### Instalação por linha de comando

Use o seguinte comando de exemplo para instalar ou atualizar o site:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
controller,desktopstudio,licenseserver,director /configure_firewall /
quiet /enable_new_monitoring_features
```

### Etapas de reversão

1. Certifique-se de fazer o backup do banco de dados de Monitoramento.
2. Baixe e execute o script de reversão do banco de dados chamado dbollback.zip.

> **Observação:**
>
> O script PowerShell (`dbrollback.ps1`) incluído no arquivo `dbrollback.zip` mostra como executar o script rollback.sql se o sqlcmd estiver instalado no DDC.

3. Restaure o banco de dados de monitoramento a partir do backup que você já fez. Para obter mais informações, consulte o artigo de compartilhamento de conhecimento CTX135207.
4. Desinstale o seguinte do Painel de Controle:
   - Selecione **Citrix Monitor Service PowerShell Snap-in- x64** e clique em **Desinstalar**.
   - Selecione **Citrix Monitor Service - x64** e clique em **Desinstalar**.
   - Selecione **Citrix Director** e clique em **Desinstalar**.
5. Reinstale o Delivery Controller e o Director usando o instalador do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte instalar componentes principais

   Ou,

   Você também pode reinstalar os componentes usando o seguinte comando:

   ```
   XenDesktopServerSetup.exe /components controller,director /
   configure_firewall /quiet
   ```

6. Certifique-se de que a caixa de seleção **Instalar Director Current Release** `<version>` não esteja selecionada.
7. Após a conclusão da instalação, selecione a caixa de seleção **Abrir Citrix Site Manager**.
8. Execute uma atualização do site se sugerido no Citrix Site Manager.

## Suporte e conformidade

### Suporte

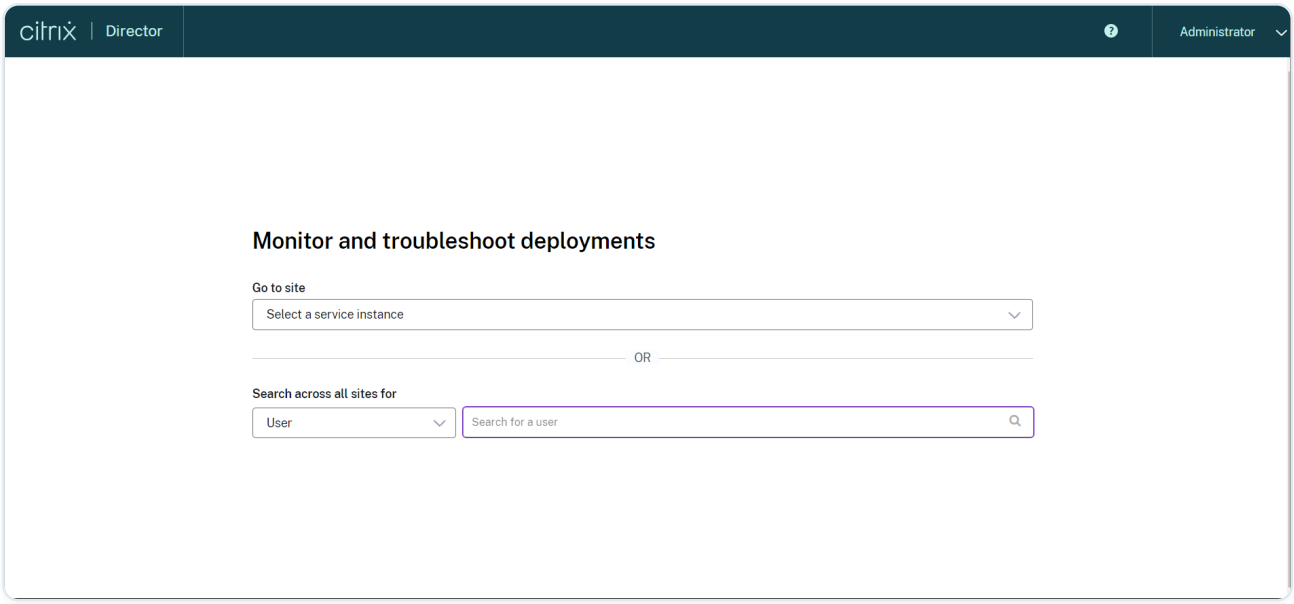
- As versões do Director do Cumulative Release (CR) são compatíveis com LTSR, mas não estão em conformidade com LTSR.
- Após a atualização, todos os tickets de suporte e correções de bugs necessários são adicionados ao seguinte Cumulative Release (CR) para o Director.
- O CR com as alterações ou correções é disponibilizado nas seguintes Atualizações Cumulativas (CU).

### 508/WCAG 2.1

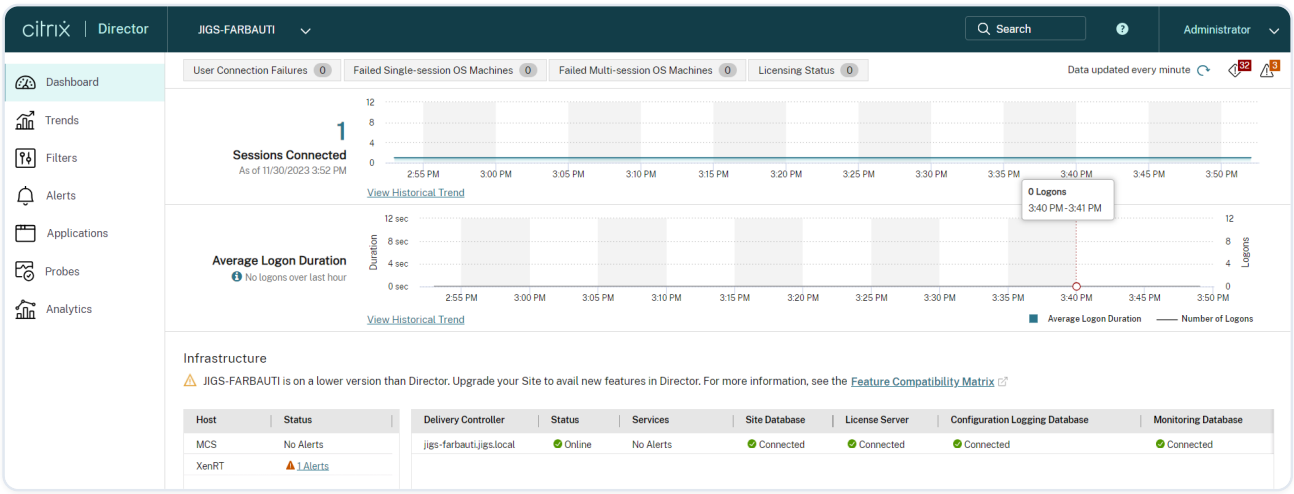
- Para clientes com o mandato de conformidade 508/WCAG 2.1, recomenda-se continuar a usar a versão LTSR de todos os componentes principais.

# Análise do Site

Usando o Director, você pode monitorar a saúde de suas implantações. Você pode solucionar problemas de desempenho pesquisando por um usuário, endpoint ou máquina em todos os sites integrados.




Com permissão total de administrador, ao abrir o Director, o Painel fornece um local centralizado para monitorar a integridade e o uso de um site.




Se não houver falhas atualmente e nenhuma falha tiver ocorrido nos últimos 60 minutos, os painéis permanecem recolhidos. Quando há falhas, o painel de falha específico aparece automaticamente.

> **Observação:**
>
> Dependendo da licença da sua organização e dos seus privilégios de Administrador, algumas opções ou recursos podem não estar disponíveis.

# Painéis no Painel do Director

## Falhas de Conexão do Usuário

Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para visualizar as métricas para esse tipo de falha. Na tabela adjacente, esse número é detalhado por grupos de entrega. As falhas de conexão incluem falhas causadas pelo atingimento dos limites do aplicativo. Para obter mais informações sobre os limites do aplicativo, consulte Aplicativos.

## Máquinas OS de sessão única com falha ou Máquinas OS de várias sessões com falha

Total de falhas nos últimos 60 minutos, detalhadas por grupos de entrega. Falhas detalhadas por tipo, incluindo falha ao iniciar, travado na inicialização e não registrado. Para máquinas com SO de múltiplas sessões, as falhas também incluem máquinas que atingem a carga máxima.

## Status de Licenciamento

Os alertas do License Server exibem alertas enviados pelo License Server e as ações necessárias para resolvê-los. Requer License Server Versão 11.12.1 ou posterior. Os alertas do Delivery Controller exibem os detalhes do estado de licenciamento conforme visto pelo Controller e são enviados pelo Controller. Requer Controller para XenApp 7.6 ou XenDesktop 7.6 ou posterior. Você pode definir o limite para alertas no Studio. O status de licenciamento exibido em **Delivery Controllers** > **Detalhes** > **Edições do Produto** > **PLT** indica **Premium** e não **Platinum**.

## Estado de Carência

O Director exibe um dos seguintes estados de carência. Esta informação é obtida do Delivery Controller.

1. **Não Ativo:** Não está em nenhum tipo de modo de cache de licença. Os limites normais de licenciamento se aplicam.
2. **Carência de Emergência:** Entra em vigor quando o servidor de licenças está inacessível ou as informações de licença não podem ser obtidas durante a intermediação de uma conexão. Os usuários não são afetados. Os erros mostrados no Director não podem ser ignorados até que o servidor de licenças esteja acessível.
3. **Graça Expirada:** O modo de cache de licença de emergência expirou.

Para obter mais informações, consulte Excesso de licenças e Modo de intermitência de licenças.

### Sessões Conectadas

Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.

### Duração Média do Logon

Dados de logon dos últimos 60 minutos. O número grande à esquerda é a duração média do logon ao longo da hora. Os dados de logon para VDAs anteriores ao XenDesktop 7.0 não estão incluídos nesta média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

### Infraestrutura

Lista a infraestrutura do seu site - hosts e Controladores. Para infraestrutura do XenServer ou VMware, você pode visualizar alertas de desempenho. Por exemplo, você pode configurar o XenCenter para gerar alertas de desempenho quando o uso da CPU, E/S de rede ou E/S de disco exceder um limite especificado em um servidor gerenciado ou máquina virtual. Por padrão, o intervalo de repetição do alerta é de 60 minutos, mas você também pode configurá-lo. Para obter detalhes, consulte a seção Alertas de Desempenho do XenCenter na documentação do produto XenServer.

> **Observação:**

> Se nenhum ícone aparecer para uma métrica específica, isso indica que essa métrica não é suportada pelo tipo de host que você está usando. Por exemplo, nenhuma informação de saúde está disponível para hosts do System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

> Continue a solucionar problemas usando estas opções (que estão documentadas nas seções a seguir):

- Controlar energia da máquina do usuário
- Impedir conexões com máquinas

## Monitorar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| Visualizar a máquina ou sessão atualmente conectada de um usuário | Nas exibições Gerenciador de Atividades e Detalhes do Usuário, visualize a máquina ou sessão atualmente conectada do usuário e uma lista de todas as máquinas e sessões às quais este usuário tem acesso. Para acessar esta lista, clique no ícone do alternador de sessão na barra de título do usuário. Para obter mais informações, consulte Restaurar sessões. |
| Visualizar o número total de sessões conectadas em todos os grupos de entrega | No Painel, no painel **Sessões Conectadas**, visualize o número total de sessões conectadas em todos os grupos de entrega nos últimos 60 minutos. Em seguida, clique no grande número total, que abre a exibição Filtros, onde você pode exibir dados gráficos de sessão com base em grupos de entrega e intervalos selecionados e uso em todos os grupos de entrega. |
| Encerrar sessões ociosas | A exibição Filtros de Sessões exibe dados relacionados a todas as sessões ativas. Filtre as sessões com base no Usuário Associado, grupo de entrega, Estado da Sessão e Tempo Ocioso maior que um período de tempo limite. Na lista filtrada, selecione as sessões para fazer logoff ou desconectar. Para obter mais informações, consulte Solucionar problemas de aplicativos. |
| Visualizar dados por um período de tempo mais longo | Na exibição Tendências, selecione a guia **Sessões** para detalhar dados de uso mais específicos para sessões conectadas e desconectadas por um período de tempo mais longo (ou seja, totais de sessões anteriores aos últimos 60 minutos). Para visualizar essas informações, clique em **Visualizar tendências históricas**. |

**Observação:**

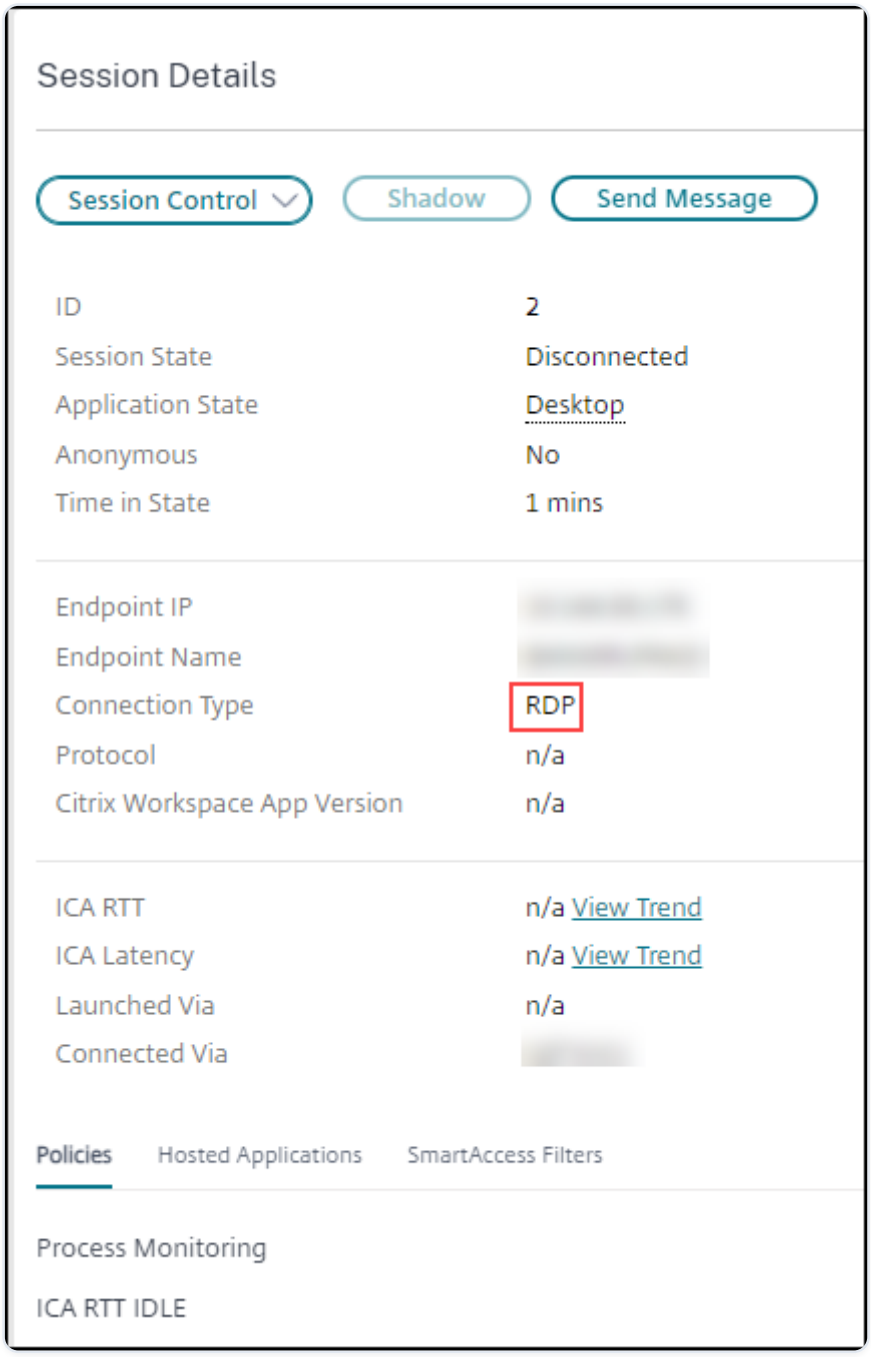
Se o dispositivo do usuário estiver executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7, ou um VDA Linux, o Director não poderá exibir informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem informando que as informações não estão disponíveis.

**Limitação das Regras de Atribuição de Desktop:** O Web Studio permite a atribuição de várias Regras de Atribuição de Desktop (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront™ exibe o desktop atribuído com o **Nome de Exibição** correspondente de acordo com a DAR para o usuário logado. No entanto, o Director não suporta DARs e exibe o desktop atribuído usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear um desktop específico para uma máquina no Director. Você pode mapear o desktop atribuído exibido no StoreFront para o nome do grupo de entrega exibido no Director usando o seguinte comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

### Protocolo de transporte da sessão

Visualize o protocolo de transporte em uso para o tipo de conexão HDX para a sessão atual no painel **Detalhes da Sessão**. Esta informação está disponível para sessões iniciadas em VDAs Versão 7.13 ou posterior.




- Para o tipo de conexão **HDX™**,
  - O Protocolo é exibido como **UDP**, se EDT for usado para a conexão HDX.
  - O Protocolo é exibido como **TCP**, se TCP for usado para a conexão HDX.
- Para o tipo de conexão **RDP**, o Protocolo é exibido como **n/a**.

Quando o transporte adaptável está configurado, o protocolo de transporte da sessão alterna dinamicamente entre EDT (sobre UDP) e TCP, com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ela retorna ao protocolo TCP.

Para obter mais informações sobre a configuração do transporte adaptativo, consulte Transporte Adaptativo.

## Exportar relatórios

Você pode exportar dados de tendências para gerar relatórios regulares de uso e gerenciamento de capacidade. A exportação suporta os formatos de relatório PDF, Excel e CSV. Relatórios nos formatos PDF e Excel contêm tendências representadas como gráficos e tabelas. Relatórios no formato CSV contêm dados tabulares que podem ser processados para gerar visualizações ou podem ser arquivados.

Para exportar um relatório:

1. Vá para a guia **Tendências**.
2. Defina os critérios de filtro e o período e clique em **Aplicar**. O gráfico de tendências e a tabela são preenchidos com dados.
3. Clique em **Exportar** e insira o nome e o formato do relatório.

O Director gera o relatório com base nos critérios de filtro selecionados. Se você alterar os critérios de filtro, clique em **Aplicar** antes de clicar em **Exportar**.

> **Observação:**
>
> A exportação de uma grande quantidade de dados causa um aumento significativo no consumo de memória e CPU nos servidores Director, Delivery Controller e SQL. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados são definidos para limites padrão para obter um desempenho de exportação ideal.

### Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos para os critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados além dos limites padrão no número de linhas ou registros na tabela. O número padrão de registros suportados é definido com base no formato do relatório.

Você pode alterar o limite padrão configurando as Configurações do Aplicativo Director no Internet Information Services (IIS).

| FORMATO DO RELATÓRIO | NÚMERO PADRÃO DE REGISTROS SUPORTADOS | CAMPOS NAS CONFIGURAÇÕES DO APLICATIVO DIRECTOR | NÚMERO MÁXIMO DE REGISTROS SUPORTADOS |
|---|---|---|---|
| PDF | 500 | UI.ExportPdfDrilldownLimit | 5000 |
| Excel | 100.000 | UI.ExportExcelDrilldownLimit | 100.000 |
| CSV | 100.000 (10.000.000 na guia **Sessões**) | UI.ExportCsvDrilldownLimit | 100.000 |

Para alterar o limite do número de registros que você pode exportar:

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Default website.
3. Clique duas vezes em **Application Settings**.
4. Edite ou adicione uma configuração para os campos UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit ou UI.ExportCsvDrilldownLimit, conforme necessário.

Adicionar esses valores de campo em Application Settings substitui os valores padrão.

> **Aviso:**
>
> Definir valores de campo maiores que o número máximo de registros suportados pode afetar o desempenho da Exportação e não é suportado.

### Tratamento de Erros

Esta seção fornece informações sobre como lidar com erros que você pode encontrar durante a operação de Exportação.

- **O Director atingiu o tempo limite**

Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos no servidor Director ou com o Serviço Monitor.

A duração padrão do tempo limite é de 100 segundos. Para aumentar a duração do tempo limite do Serviço Director, defina o valor do campo **Connector.DataServiceContext.Timeout field in** nas Configurações do Aplicativo Director no Internet Information Services (IIS):

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Sites Padrão.
3. Clique duas vezes em **Application Settings**.
4. Edite o valor **Connector.DataServiceContext.Timeout**.

- **O Monitor atingiu o tempo limite**

Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos com o Serviço Monitor ou no servidor SQL.

Para aumentar a duração do tempo limite do Serviço Monitor, execute os seguintes comandos PowerShell no Delivery Controller:

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **Operações de Exportação ou Visualização simultâneas máximas em andamento**

O Director suporta uma instância de Exportação ou Visualização. Se você receber o erro **Operações de Exportação ou Visualização simultâneas máximas em andamento**, tente a próxima operação de Exportação novamente mais tarde.

É possível aumentar o número de operações simultâneas de Exportar ou Visualizar, no entanto, isso pode afetar o desempenho do Director e não é suportado:

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director sob o site padrão.
3. Clique duas vezes em **Configurações do Aplicativo**.
4. Edite o valor **UI.ConcurrentExportLimit**.

- **Espaço em disco insuficiente no Director**

Cada operação de Exportação requer um máximo de 2 GB de espaço em disco rígido na pasta Temp do Windows. Tente a Exportação novamente após liberar espaço ou adicionar mais espaço em disco rígido no servidor Director.

## Hotfixes do Monitor

Para visualizar os hotfixes instalados em um VDA de máquina específico (físico ou VM), escolha a exibição **Detalhes da Máquina**.

## Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas que você seleciona no Director, use as opções de Controle de Energia. Essas opções estão disponíveis para máquinas de SO de sessão única, mas podem não estar disponíveis para máquinas de SO de múltiplas sessões.

**Observação:**

Esta funcionalidade não está disponível para máquinas físicas ou máquinas que usam o Acesso Remoto a PC.

| COMANDO | FUNÇÃO |
| --- | --- |
| **Reiniciar** | Executa um desligamento ordenado (suave) da VM e todos os processos em execução são interrompidos individualmente antes de reiniciar a VM. Por exemplo, selecione máquinas que aparecem no Director como "falha ao iniciar" e use este comando para reiniciá-las. |
| **Forçar Reinício** | Reinicia a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico e depois conectá-lo novamente e ligá-lo. |
| **Desligar** | Executa um desligamento ordenado (suave) da VM. Todos os processos em |

| COMANDO | FUNÇÃO |
| --- | --- |
| | execução são interrompidos individualmente. |
| **Forçar Desligamento** | Desliga a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico. Nem sempre pode desligar todos os processos em execução, e você corre o risco de perder dados se desligar uma VM dessa forma. |
| **Suspender** | Suspende uma VM em execução em seu estado atual e armazena esse estado em um arquivo no repositório de armazenamento padrão. Esta opção permite que você desligue o servidor host da VM e, posteriormente, após reiniciá-lo, retome a VM, retornando-a ao seu estado de execução original. |
| **Retomar** | Retoma uma VM suspensa e restaura seu estado de execução original. |
| **Iniciar** | Inicia uma VM quando ela está desligada (também conhecido como inicialização a frio). |

Se as ações de controle de energia falharem, passe o mouse sobre o alerta e uma mensagem pop-up aparecerá com detalhes sobre a falha.

## Impedir conexões a máquinas

Use o modo de manutenção para impedir novas conexões temporariamente enquanto o administrador apropriado executa tarefas de manutenção na imagem.

Quando você habilita o modo de manutenção nas máquinas, nenhuma nova conexão é permitida até que você o desabilite. Se os usuários estiverem atualmente logados, o modo de manutenção entra em vigor assim que todos os usuários fizerem logoff. Para usuários que não fizerem logoff,

envie uma mensagem informando-os de que as máquinas serão desligadas em um determinado horário e use os controles de energia para forçar o desligamento das máquinas.

1. Selecione a máquina, como na exibição Detalhes do Usuário, ou um grupo de máquinas na exibição Filtros.
2. Selecione **Modo de Manutenção** e ative a opção.

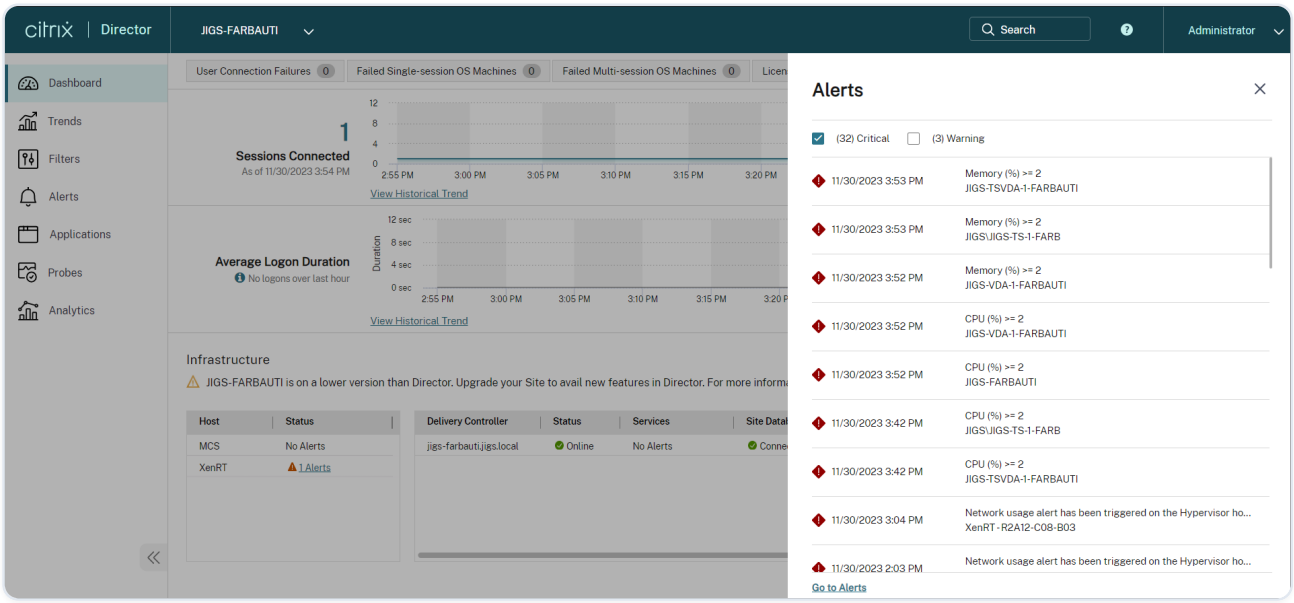
Se um usuário tentar se conectar a um desktop atribuído enquanto ele estiver no modo de manutenção, uma mensagem aparece indicando que o desktop está indisponível. Nenhuma nova conexão pode ser feita até que você desative o modo de manutenção.

## Análise de Aplicativos

A guia **Aplicativos** exibe análises baseadas em aplicativos em uma visualização única e consolidada para ajudar a analisar e gerenciar o desempenho do aplicativo de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. Ele mostra métricas como os resultados da sondagem, o número de instâncias por aplicativo e as falhas e erros associados aos aplicativos publicados. Para obter mais informações, consulte a seção Análise de Aplicativos em **Solução de Problemas de Aplicativos**.

## Alertas e notificações

Alertas são exibidos no Director no painel e em outras visualizações de alto nível com símbolos de alerta de aviso e críticos. Alertas estão disponíveis para sites com licença **Premium**. Os alertas são atualizados automaticamente a cada minuto; você também pode atualizar os alertas sob demanda.

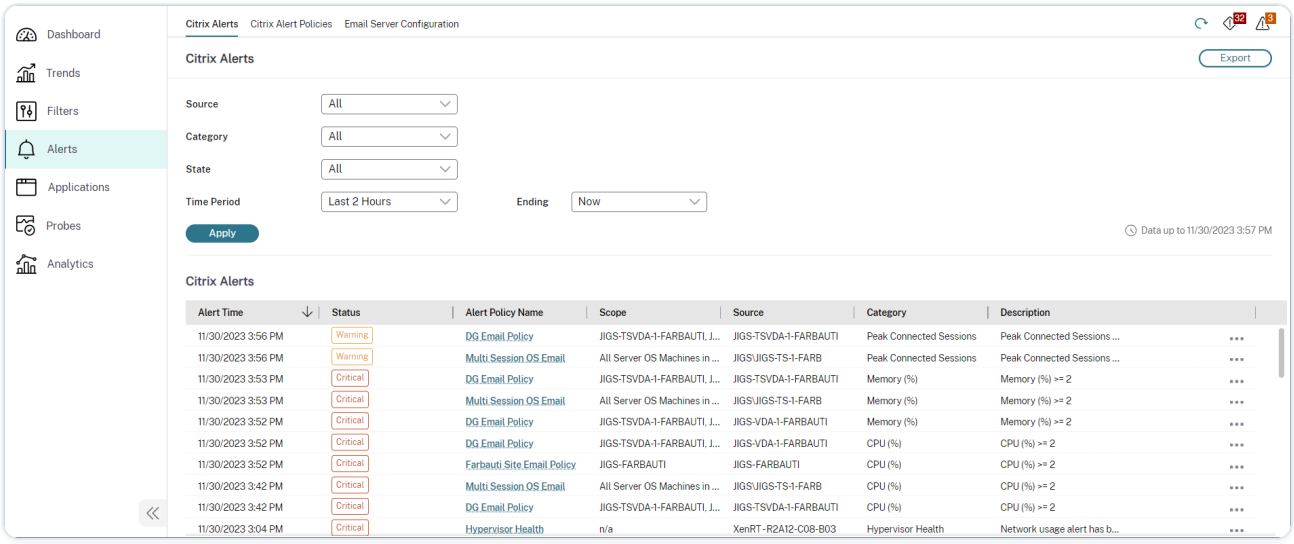


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre os alertas selecionando um alerta na barra lateral, clicando no link **Ir para Alertas** na parte inferior da barra lateral ou selecionando **Alertas** na parte superior da página do Director.

Na exibição de Alertas, você pode filtrar e exportar alertas. Por exemplo, máquinas de SO multi-sessão com falha para um Grupo de Entrega específico no último mês, ou todos os alertas para um usuário específico. Para obter mais informações, consulte Exportar relatórios.




## Alertas Citrix®

Os alertas Citrix são alertas monitorados no Director que se originam de componentes Citrix. Você pode configurar alertas Citrix dentro do Director em **Alertas** \> **Política de Alertas Citrix**. Como parte da configuração, você pode definir notificações para serem enviadas por e-mail a indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar Alertas Citrix, consulte Criar políticas de alerta.

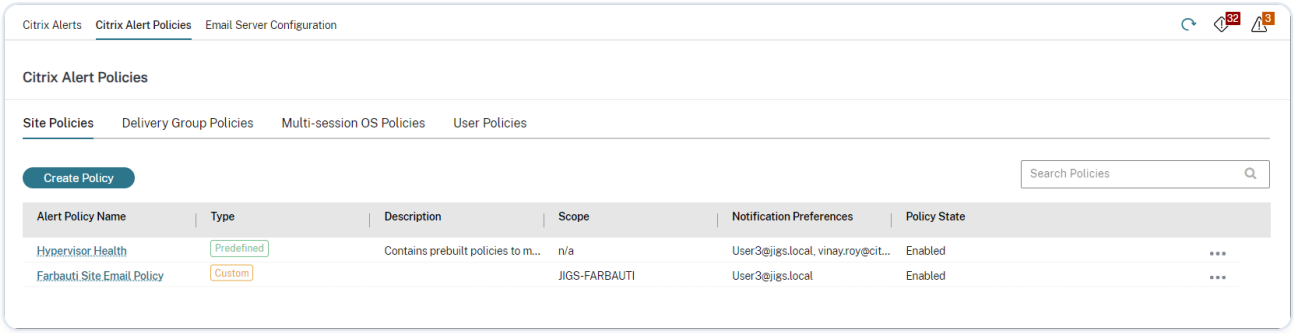
> **Observação:**
>
> Certifique-se de que seu firewall, proxy ou Microsoft Exchange Server não bloqueie os alertas de e-mail.

## Políticas de alerta inteligentes

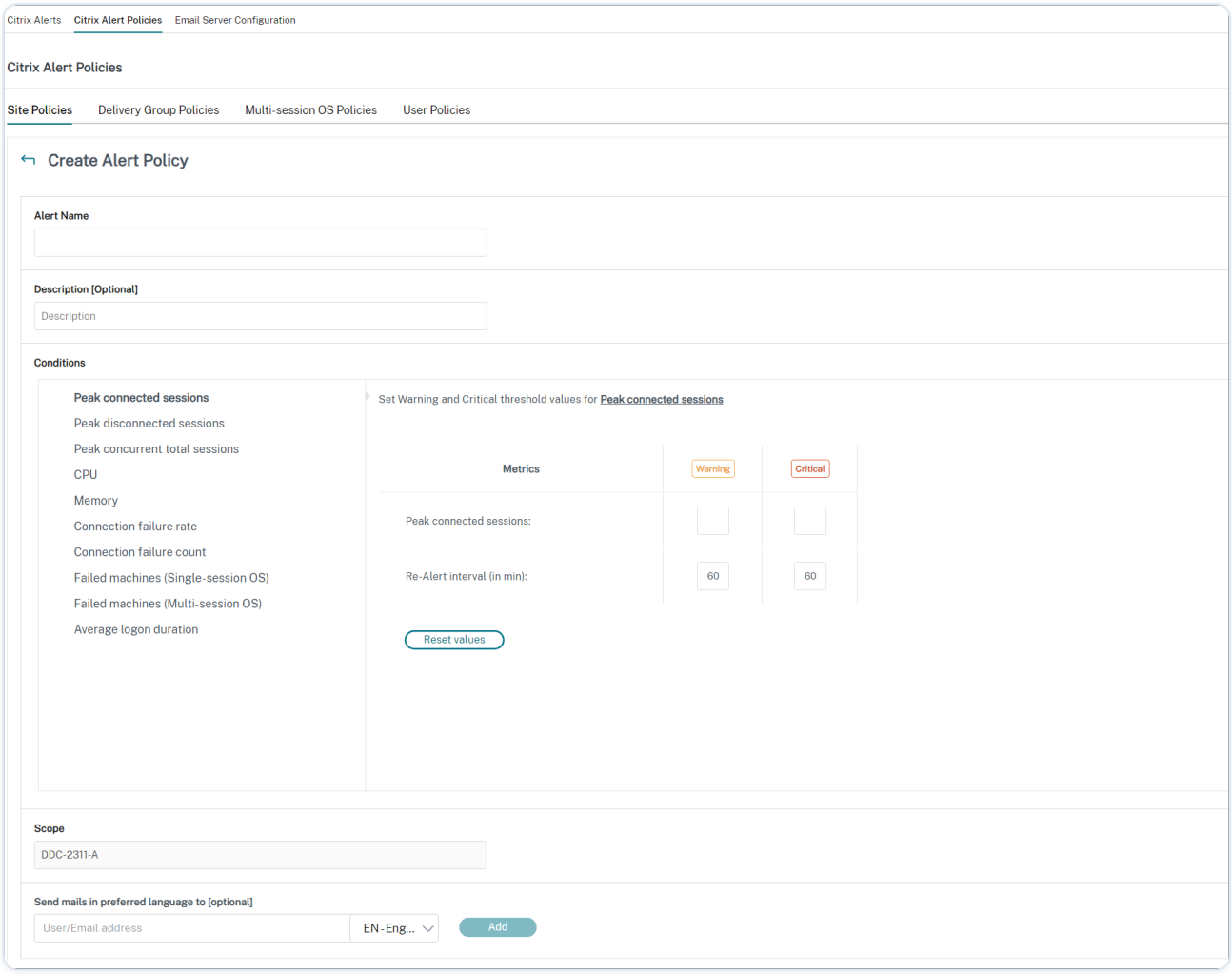
Um conjunto de políticas de alerta integradas com valores de limite predefinidos está disponível para Grupos de Entrega e escopo de VDA de SO multi-sessão. Este recurso requer a versão 7.18 ou posterior do(s) Delivery Controller(s). Você pode modificar os parâmetros de limite das políticas de alerta integradas em **Alertas** \> **Política de Alertas Citrix**. Essas políticas são criadas quando há pelo menos um destino de alerta — um Grupo de Entrega ou um VDA de SO multi-sessão definido em seu site. Além disso, esses alertas integrados são adicionados automaticamente a um novo grupo de entrega ou a um VDA de SO multi-sessão.

Caso você atualize o Director e seu site, as políticas de alerta da sua instância anterior do Director são transferidas. As políticas de alerta integradas são criadas somente se não existirem regras de alerta correspondentes no banco de dados do Monitor.

Para os valores de limite das políticas de alerta integradas, consulte a seção Condições das políticas de alerta.



## Criar políticas de alerta




Para criar uma nova política de alertas, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alertas** > **Política de Alertas Citrix** e selecione, por exemplo, Política de SO multi-sessão.
2. Clique em **Criar**.
3. Nomeie e descreva a política, depois defina as condições que devem ser atendidas para que o alerta seja acionado. Por exemplo, especifique as contagens de Aviso e Crítico para Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico. Os valores de Aviso não devem ser maiores que os valores Críticos. Para obter mais informações, consulte Condições das políticas de alerta.
4. Defina o intervalo de Re-alerta. Se as condições para o alerta ainda forem atendidas, o alerta será acionado novamente neste intervalo de tempo e, se configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta ignorado não gera uma notificação por e-mail no intervalo de re-alerta.
5. Defina o Escopo. Por exemplo, defina para um Grupo de Entrega específico.

6. Em Preferências de notificação, especifique quem deve ser notificado por e-mail quando o alerta for acionado. Você deve especificar um servidor de e-mail na guia **Configuração do Servidor de E-mail** para definir as preferências de Notificação por e-mail nas Políticas de Alerta.
7. Clique em **Salvar**.

A criação de uma política com 20 ou mais Grupos de Entrega definidos no Escopo pode levar aproximadamente 30 segundos para concluir a configuração. Um indicador de carregamento é exibido durante esse tempo.

A criação de mais de 50 políticas para até 20 Grupos de Entrega exclusivos (1000 destinos de Grupo de Entrega no total) pode resultar em um aumento no tempo de resposta (mais de 5 segundos).

Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro pode acionar alertas errôneos de Grupo de Entrega que são definidos usando parâmetros de máquina.

> **Nota:** Depois de excluir uma política de alerta, pode levar até 30 minutos para que as notificações de alerta geradas pela política parem.

## Condições das políticas de alertas

Encontre abaixo as categorias de alerta, as ações recomendadas para mitigar o alerta e as condições de política integradas, se definidas. As políticas de alerta integradas são definidas para intervalos de alerta e realerta de 60 minutos.

### Pico de Sessões Conectadas

- Verifique a exibição Tendências de Sessão do Director para o pico de sessões conectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário

### Pico de Sessões Desconectadas

- Verifique a exibição Tendências de Sessão do Director para o pico de sessões desconectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário

### Pico de Sessões Desconectadas

- Verifique a exibição Tendências de Sessão do Director no Director para o pico de sessões concorrentes.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

### Pico de Sessões Totais Concorrentes

- Verifique a exibição Tendências de Sessão do Director no Director para sessões simultâneas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

### CPU

A porcentagem de uso da CPU indica o consumo geral da CPU no VDA, incluindo o dos processos. Você pode obter mais informações sobre a utilização da CPU por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem CPU. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Encerrar o processo faz com que os dados não salvos sejam perdidos.
- Se tudo estiver funcionando como esperado, adicione recursos de CPU adicionais no futuro.

> **Nota:**
>
> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se essa configuração de política estiver desabilitada, alertas com condições de CPU e memória não serão acionados. Para obter mais informações, consulte Configurações de política de monitoramento

> **Condições de política inteligente:**

- **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
- **Valores de limite:** Aviso - 80%, Crítico - 90%

### Memória

A porcentagem de uso da memória indica o consumo geral de memória no VDA, incluindo o dos processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Visualizar Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem memória. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Encerrar o processo causa a perda de dados não salvos.
- Se tudo estiver funcionando como esperado, adicione memória adicional no futuro.

> **Nota:**
>
> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se essa configuração de política estiver desabilitada, alertas com condições de CPU e memória não serão acionados. Para obter mais informações, consulte Configurações de política de monitoramento

> **Condições de política inteligente:**

- **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
- **Valores de limite:** Aviso - 80%, Crítico - 90%

### Taxa de Falha de Conexão

Porcentagem de falhas de conexão na última hora.

- Calculado com base no total de falhas em relação ao total de conexões tentadas.
- Verifique a exibição Tendências de Falhas de Conexão do Director para eventos registrados no log de Configuração.

- Determine se aplicativos ou desktops estão acessíveis.

### Contagem de Falhas de Conexão

Número de falhas de conexão na última hora.

- Verifique a exibição Tendências de Falhas de Conexão do Director para eventos registrados no log de Configuração.
- Determine se aplicativos ou desktops estão acessíveis.

### ICA® RTT (Média)

Tempo médio de ida e volta do ICA.

- Verifique o Citrix ADM para uma análise detalhada do ICA RTT para determinar a causa raiz. Para obter mais informações, consulte a documentação Citrix ADM.
- Se o Citrix ADM não estiver disponível, verifique a exibição Detalhes do Usuário do Director para o ICA RTT e Latência, e determine se é um problema de rede ou um problema com aplicativos ou desktops.

### ICA RTT (Nº de Sessões)

Número de sessões que excedem o tempo de ida e volta ICA limite.

- Verifique o Citrix ADM para o número de sessões com ICA RTT alto. Para obter mais informações, consulte a documentação Citrix ADM.
- Se o Citrix ADM não estiver disponível, trabalhe com a equipe de rede para determinar a causa raiz.

  **Condições da política inteligente:**

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 300 ms para 5 ou mais sessões, Crítico - 400 ms para 10 ou mais sessões

### RTT ICA (% de Sessões)

Porcentagem de sessões que excedem o tempo médio de ida e volta ICA.

- Verifique o Citrix ADM para o número de sessões com ICA RTT alto. Para obter mais informações, consulte a documentação Citrix ADM.
- Se o Citrix ADM não estiver disponível, trabalhe com a equipe de rede para determinar a causa raiz.

### RTT ICA (Usuário)

Tempo de ida e volta ICA que é aplicado às sessões iniciadas pelo usuário especificado. O alerta é acionado se o RTT ICA for maior que o limite em pelo menos uma sessão.

### Máquinas com Falha (SO de sessão única)

Número de máquinas de SO de sessão única com falha. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz.

  **Condições de política inteligente:**

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 1, Crítico - 2

### Máquinas com falha (SO multiusuário)

Número de máquinas de SO multi-sessão com falha. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz.

  **Condições de política inteligente:**

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 1, Crítico - 2

### Máquinas com falha (em %)

Porcentagem de máquinas de SO de sessão única e multi-sessão com falha em um grupo de entrega, calculada com base no número de máquinas com falha. Esta condição de alerta permite configurar limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega e é calculada a cada 30 segundos. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director. Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Solucionar problemas do usuário.

### Duração Média de Logon

Duração média do logon para logons que ocorreram na última hora.

- Verifique o Painel do Director para obter métricas atualizadas sobre a duração do logon. Um grande número de usuários fazendo logon em um curto período de tempo pode aumentar a duração do logon.

- Verifique a linha de base e o detalhamento dos logons para restringir a causa. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

  **Condições de política inteligente:**

  - **Escopo:** Grupo de Entrega, escopo do SO de múltiplas sessões
  - **Valores limite:** Aviso - 45 segundos, Crítico - 60 segundos

**Duração do Logon (Usuário)**

Duração do logon para logons do usuário especificado que ocorreram na última hora.

**Índice do Avaliador de Carga**

Valor do Índice do Avaliador de Carga nos últimos 5 minutos.

- Verifique o Director para Máquinas de SO de múltiplas sessões que possam ter uma carga de pico (Carga máxima). Visualize o Dashboard (falhas) e o relatório de Tendências do Índice do Avaliador de Carga.

  **Condições de política inteligente:**

  - **Escopo:** Grupo de Entrega, escopo do SO de múltiplas sessões
  - **Valores de limite:** Aviso - 80%, Crítico - 90%

### Monitoramento de Alertas de Hypervisor

O Director exibe alertas para monitorar a integridade do hipervisor. Alertas do XenServer® e VMware vSphere ajudam a monitorar parâmetros e estados do hipervisor. O status da conexão com o hipervisor também é monitorado para fornecer um alerta se o cluster ou pool de hosts for reiniciado ou ficar indisponível.

Filtro de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hypervisor_alerts_filter.png)

Para receber alertas do hipervisor, certifique-se de que uma conexão de hospedagem seja criada no Web Studio. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas para alertas do hipervisor.

Esses alertas são exibidos assim que os limites são atingidos ou excedidos. Os alertas do hipervisor podem ser:

- Crítico — limite crítico da política de alarme do hipervisor atingido ou excedido
- Aviso — limite de aviso da política de alarme do hipervisor atingido ou excedido

- Ignorado — alerta não mais exibido como um alerta ativo

Exibição de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hypervisor_alerts_display.png)

Este recurso requer o Delivery Controller™ versão 7 1811 ou posterior. Se você estiver usando uma versão mais antiga do Director com sites 7 1811 ou posterior, apenas a contagem de alertas do hipervisor será exibida. Para visualizar os alertas, você deve atualizar o Director.

A tabela a seguir descreve os vários parâmetros e estados dos alertas do Hypervisor.

| ALERTA | HYPERVISORES SUPORTADOS | ACIONADO POR | CONDIÇÃO | CONFIGURAÇÃO |
|---|---|---|---|---|
| Uso da CPU | XenServer, VMware vSphere | Hypervisor | O limite de alerta de uso da CPU é atingido ou excedido | Os limites de alerta devem ser configurados no Hypervisor. |
| Uso de memória | XenServer, VMware vSphere | Hypervisor | O limite de alerta de uso de memória é atingido ou excedido | Os limites de alerta devem ser configurados no Hypervisor. |
| Uso de rede | XenServer, VMware vSphere | Hypervisor | O limite de alerta de uso de rede é atingido ou excedido | Os limites de alerta devem ser configurados no Hypervisor. |
| Uso de disco | VMware vSphere | Hypervisor | O limite de alerta de uso de disco é atingido ou excedido | Os limites de alerta devem ser configurados no Hypervisor. |
| Conexão do host ou estado de energia | VMware vSphere | Hypervisor | O Host do Hypervisor foi reiniciado ou | Os alertas são pré-construídos no VMware vSphere. Nenhuma |

| ALERTA | HYPERVISORES SUPORTADOS | ACIONADO POR | CONDIÇÃO | CONFIGURAÇÃO |
|---|---|---|---|---|
| | | | está indisponível | configuração adicional é necessária. |
| Conexão do Hypervisor indisponível | XenServer, VMware vSphere | Delivery Controller | A conexão com o hypervisor (pool ou cluster) foi perdida, desligada ou reiniciada. Este alerta é gerado a cada hora enquanto a conexão estiver indisponível. | Os alertas são pré-construídos com o Delivery Controller. Nenhuma configuração adicional é necessária. |

**Nota:**

Para obter mais informações sobre a configuração de alertas, consulte Alertas do Citrix XenCenter ou verifique a documentação de Alertas do VMware vCenter.

A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > Site Policy > Hypervisor Health**. As condições de limite para políticas de alerta do Hypervisor podem ser configuradas, editadas, desabilitadas ou excluídas apenas do hipervisor e não do Director. No entanto, a modificação das preferências de e-mail e o descarte de um alerta podem ser feitos no Director. Você pode desabilitar o alerta se sua função não envolver o monitoramento da infraestrutura.

**Importante:**

- Os alertas acionados pelo Hypervisor são buscados e exibidos no Director. No entanto, as alterações no ciclo de vida/estado dos alertas do Hypervisor não são refletidas no Director.
- Alertas que estão saudáveis ou foram dispensados ou desabilitados no console do Hypervisor continuam a aparecer no Director e precisam ser dispensados explicitamente.
- Alertas que são dispensados no Director não são dispensados automaticamente no console do Hypervisor.

## Filtrar dados para solucionar falhas

Quando você clica em números no Painel ou seleciona um filtro predefinido no menu Filtros, a exibição Filtros é aberta para exibir dados com base na máquina ou tipo de falha selecionado.

Filtros predefinidos não podem ser editados, mas você pode salvar um filtro predefinido como um filtro personalizado e depois modificá-lo. Além disso, você pode criar exibições filtradas personalizadas de máquinas, conexões, sessões e instâncias de aplicativos em todos os grupos de entrega.

1. Selecione uma exibição:

   - **Máquinas**. Selecione Máquinas de SO de sessão única ou Máquinas de SO de múltiplas sessões. Essas exibições mostram o número de máquinas configuradas. A guia Máquinas de SO de múltiplas sessões também inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.
   - **Sessões**. Você também pode ver a contagem de sessões na exibição Sessões. Use as medições de tempo ocioso para identificar sessões que estão ociosas além de um período de tempo limite. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário. Clicar no nome do **Endpoint** abre o Gerenciador de Atividades para o Endpoint. Clicar em **Exibir Detalhes** abre a página **Detalhes do Usuário** ou **Detalhes do Endpoint**, respectivamente. Para obter mais informações, consulte Detalhes do Usuário.
   - **Conexões**. Filtre as conexões por diferentes períodos de tempo, incluindo os últimos 60 minutos, as últimas 24 horas ou os últimos 7 dias.
   - **Instâncias de Aplicativo**. Esta exibição mostra as propriedades de todas as instâncias de aplicativo em VDAs de Servidor e SO de sessão única. As medições de tempo ocioso da sessão estão disponíveis para instâncias de aplicativo em VDAs de SO de múltiplas sessões.

**Nota:**

Se você iniciou sessões de Desktop em VDAs instalados em um computador Windows 10 1809, o Gerenciador de Atividades no Director pode, às vezes, exibir o Microsoft Edge e o Office como aplicativos em execução ativa, enquanto eles estão, na verdade, sendo executados apenas em segundo plano.

2. Para **Filtrar por**, selecione os critérios.
3. Use as guias adicionais para cada exibição, conforme necessário, para completar o filtro.
4. Selecione colunas extras, conforme necessário, para solucionar problemas adicionais.
5. Salve e nomeie seu filtro.
6. Para acessar filtros de vários servidores Director, armazene os filtros em uma pasta compartilhada acessível a partir desses servidores:
   - A pasta compartilhada deve ter permissões de modificação para as contas no servidor Director.
   - Os servidores Director devem ser configurados para acessar a pasta compartilhada. Para configurar, execute o **IIS Manager**. Em **Sites \> Default Web Site \> Director\ > Application Settings**, modifique a configuração **Service.UserSettingsPath** para refletir o caminho UNC da pasta compartilhada.
7. Para abrir o filtro mais tarde, no menu **Filtros**, selecione o tipo de filtro (Máquinas, Sessões, Conexões ou Instâncias de Aplicativo) e, em seguida, selecione o filtro salvo.
8. Clique em **Exportar** para exportar os dados para arquivos no formato CSV. Dados de até 100.000 registros podem ser exportados. Este recurso está disponível no Delivery Controller™ versão 1808 e posterior.
9. Se necessário, para as exibições de **Máquinas** ou **Conexões**, use os controles de energia para todas as máquinas selecionadas na lista filtrada. Para a exibição de Sessões, use os controles de sessão ou a opção de enviar mensagens.
10. Nas exibições de **Máquinas** e **Conexões**, clique em **Motivo da Falha** de uma máquina ou conexão com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de Máquina e Conexão estão disponíveis em Motivos de falha e solução de problemas do Citrix Director.

11. Na exibição de **Máquinas**, clique em um link de nome de máquina para ir para a página correspondente de **Detalhes da Máquina**. Esta página exibe os detalhes da máquina, fornece controles de energia, exibe os gráficos de monitoramento de CPU, memória, disco e GPU. Além disso, clique em **Exibir Utilização Histórica** para ver as tendências de utilização de recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
12. Na visualização **Instâncias de Aplicativo**, classifique ou filtre com base no **Tempo Ocioso** maior que um período de tempo limite. Selecione as instâncias de aplicativo ociosas para encerrar. Fazer logoff ou desconectar uma instância de aplicativo encerra todas as instâncias de aplicativo ativas na mesma sessão. Para obter mais informações, consulte Solucionar problemas de aplicativos. A página de filtro Instâncias de Aplicativo e as medições de tempo ocioso nas páginas de filtro Sessões estão disponíveis se o Director, os Delivery Controllers e os VDAs forem da versão 7.13 ou posterior.

**Nota:** O Web Studio permite a atribuição de várias Regras de Atribuição de Área de Trabalho (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront™ exibe a área de trabalho atribuída com o Nome de Exibição correspondente de acordo com a DAR para o usuário logado. No entanto, o Director não oferece suporte a DARs e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear uma área de trabalho específica para uma máquina no Director. Para mapear a área de trabalho atribuída exibida no StoreFront para o nome do grupo de entrega exibido no Director, use o seguinte comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

## Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina

- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site.

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar pelos gráficos de tendências, ampliando um período de tempo (clicando em um ponto de dados no gráfico) e detalhando para ver os detalhes associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que é afetado.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

Escolha um período de tempo para o qual você precisa das informações de tendências históricas. A disponibilidade do período de tempo depende da sua implantação do Director da seguinte forma:

- Relatórios de tendências de até o Último ano (365 dias) estão disponíveis em sites com licença Premium.
- Relatórios de tendências de até o Último mês (31 dias) estão disponíveis em sites com licença Advanced.
- Relatórios de tendências de até os Últimos 7 dias em sites sem licença Premium e sem licença Advanced.

> **Nota:**
>
> - Em todas as implantações do Director, as informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Último mês (**Terminando agora**) ou menor. Para o período escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendência estão disponíveis como gráficos e não como tabelas.
> - Os valores de retenção de limpeza do Serviço de Monitoramento controlam a disponibilidade dos dados de tendências. Os valores padrão estão disponíveis em

Granularidade e retenção de dados. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção.

- Os seguintes parâmetros no Gerenciador do IIS controlam o intervalo de datas de término personalizadas disponíveis para seleção. No entanto, a disponibilidade dos dados para as datas selecionadas depende da configuração de retenção de limpeza para a métrica específica que está sendo medida.

| PARÂMETRO | VALORES PADRÃO |
|---|---|
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

### Tendências disponíveis

**Visualizar tendências para sessões:** Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é habilitada quando as políticas de Confiabilidade da Sessão ou Reconexão Automática do Cliente estão em vigor. Quando há uma interrupção de rede no endpoint, as seguintes políticas entram em vigor:

- A confiabilidade da sessão entra em vigor (por padrão por 3 minutos) onde o Citrix Receiver™ ou o aplicativo Citrix Workspace™ tenta se conectar ao VDA.
- A reconexão automática do cliente entra em vigor entre 3 e 5 minutos, onde o cliente tenta se conectar ao VDA.

Ambas as reconexões são capturadas e exibidas ao usuário. Esta informação pode levar um tempo máximo de 5 minutos para aparecer na interface do usuário do Director após a reconexão ter ocorrido.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções. Também analisa redes com uma experiência contínua. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período

selecionado nos Filtros. Um detalhamento fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Este recurso requer Delivery Controller™ versão 7 1906 ou posterior, e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações da política de reconexão automática do cliente e Configurações da política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Director pelos seguintes motivos:

- O aplicativo Workspace não está enviando dados de reconexão automática para o VDA.
- O VDA não está enviando dados para o serviço de monitoramento.
- Os Delivery Controllers descartam cargas úteis de VDA, pois podem não ter as sessões correspondentes.

> **Nota:**
>
> Às vezes, o endereço IP do cliente pode não ser obtido corretamente se certas políticas do Citrix Gateway estiverem definidas.

> **Visualizar tendências de falhas de conexão:** Na guia Falhas, selecione a conexão, o tipo de máquina, o tipo de falha, o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em seu site.

**Visualizar tendências de falhas de máquina:** Na guia **Falhas de Máquina de SO de Sessão Única** ou na guia Máquinas de SO de Múltiplas Sessões, selecione o tipo de falha, o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de máquina em seu site.

**Visualizar tendências de desempenho de logon:** Na guia **Desempenho de Logon**, selecione o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em seu site e se o número de logons afeta o

desempenho. Esta exibição também mostra a duração média das fases de logon, como duração de corretagem e tempo de inicialização da VM. Esses dados são especificamente para logons de usuário e não incluem usuários tentando se reconectar de sessões desconectadas. A tabela abaixo do gráfico mostra a Duração do Logon por Sessão do Usuário. Você pode escolher as colunas a serem exibidas e classificar o relatório por qualquer uma das colunas. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

**Visualizar tendências de avaliação de carga:** Na guia **Índice do Avaliador de Carga**, visualize um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas de SO de Múltiplas Sessões. As opções de filtro para este gráfico incluem o Grupo de Entrega ou a máquina de SO de Múltiplas Sessões em um Grupo de Entrega, a máquina de SO de Múltiplas Sessões (disponível apenas se a máquina de SO de Múltiplas Sessões em um Grupo de Entrega foi selecionada) e o intervalo.

**Visualizar uso de aplicativos hospedados:** A disponibilidade desse recurso depende da licença da sua organização. Na guia **Gerenciamento de Capacidade**, selecione a guia **Uso de Aplicativos Hospedados**. Selecione o Grupo de Entrega e o período para visualizar um gráfico exibindo o pico de uso simultâneo e uma tabela exibindo o uso baseado em aplicativo. Na tabela Uso Baseado em Aplicativo, você pode escolher um aplicativo específico para ver detalhes e uma lista de usuários que estão usando ou usaram o aplicativo.

**Visualizar uso de SO de Sessão Única e Múltiplas Sessões:** A exibição Tendências mostra o uso de SO de Sessão Única por site e por Grupo de Entrega. Ao selecionar **Site**, o uso é mostrado por Grupo de Entrega. Ao selecionar Grupo de Entrega, o uso é mostrado por Usuário. A exibição Tendências também mostra o uso de SO de Múltiplas Sessões por site, por Grupo de Entrega e por Máquina. Ao selecionar **Site**, o uso é mostrado por Grupo de Entrega. Ao selecionar Grupo de Entrega, o uso é mostrado por Máquina e por Usuário. Quando Máquina é selecionada, o uso é mostrado por Usuário.

**Visualizar uso de máquina virtual:** Na guia **Uso da Máquina**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter uma visualização em tempo real do uso da sua VM, permitindo que você avalie rapidamente as necessidades de capacidade do seu site. Disponibilidade de SO de Sessão Única - exibe o estado atual das máquinas de SO de Sessão Única (VDIs) por disponibilidade para todo o site ou um Grupo de Entrega específico. Disponibilidade de SO de Múltiplas Sessões - exibe o estado atual das máquinas de SO de Múltiplas Sessões por disponibilidade para todo o site ou um Grupo de Entrega específico.

**Nota:** O número de máquinas exibidas no Contador Disponível inclui máquinas em modo de manutenção.

**Visualizar utilização de recursos:** Na guia **Utilização de Recursos**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter informações sobre dados de tendências históricas para uso de CPU e memória, e IOPS e latência de disco para cada máquina VDI para um melhor planejamento de capacidade. Este recurso requer Delivery Controllers e VDAs **versão 7.11** ou posterior. Os gráficos mostram dados para CPU média, memória média, IOPS médio, latência de disco e pico de sessões simultâneas. Você pode detalhar a máquina e visualizar dados e gráficos para os 10 principais processos que consomem CPU.

Filtre por Grupo de Entrega e Período. Os gráficos de uso de CPU, memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, mês e ano. Os gráficos de IOPS médio e latência de disco estão disponíveis para as últimas 24 horas, mês e ano.

**Nota:**

- A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como **Permitido** para coletar e exibir dados na tabela dos 10 Principais Processos na página Utilização Histórica da Máquina. A política é definida como **Proibido** por padrão. Todos os dados de utilização de recursos são coletados por padrão. Isso pode ser desabilitado usando a configuração da política **Habilitar Monitoramento de Recursos**. A tabela abaixo dos gráficos mostra os dados de utilização de recursos por máquina. Para obter mais informações, consulte Configurações da política de monitoramento.
- O IOPS médio mostra as médias diárias. O IOPS de pico é calculado como o maior das médias de IOPS para o intervalo de tempo selecionado. (Uma média de IOPS é a média horária de IOPS coletados durante a hora no VDA).
- O detalhamento da máquina lista processos com uso médio de CPU ou memória média superior a 1%, o que pode significar que, às vezes, menos de 10 processos são listados.

**Visualizar dados de análise de rede:** A disponibilidade desse recurso depende da licença da sua organização e das suas permissões de administrador. Este recurso requer Delivery Controllers **versão 7.11** ou posterior.

Na guia **Rede**, monitore sua análise de rede, que fornece uma visão contextual da rede para usuário, aplicativo e desktop. Com esse recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação por meio de relatórios HDX Insight do Citrix ADM. Para obter mais informações, consulte Configurar análise de rede

**Exibir falhas de aplicativo:** A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de várias sessões executando Windows Server 2008 e posterior são suportados. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas falhas de aplicativo de VDAs de SO de várias sessões são exibidas. Você pode definir o monitoramento de falhas de aplicativo usando políticas de Monitoramento. Para obter mais informações, consulte Configurações de política de monitoramento.

**Exibir resultados da sondagem:** A guia **Resultados da Sondagem** exibe os resultados da sondagem para aplicativos e desktops que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha ocorreu é registrado.

Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

**Criar relatórios personalizados:** A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados históricos e em tempo real do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatório Personalizado salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique condições de filtro com base em campos como máquina, Grupo de Entrega ou período de tempo. Especifique colunas adicionais necessárias em seu Relatório Personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta de Relatório Personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta de Relatório Personalizado com base em uma consulta OData copiada. Para fazer isso, selecione a opção Consulta OData e cole a consulta OData copiada. Você pode salvar a consulta resultante para execução posterior.

**Nota:** Os nomes das colunas nos relatórios de Visualização e Exportação gerados usando consultas OData não são localizados, mas aparecem em inglês.

Os ícones de bandeira no gráfico indicam eventos ou ações significativas para aquele intervalo de tempo específico. Passe o mouse sobre a bandeira e clique para listar eventos ou ações.

**Nota:**

- Os dados de logon de conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
- Grupos de Entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros de Tendências do Director até que os dados relacionados a eles sejam removidos. A seleção de um Grupo de Entrega excluído exibe gráficos para os dados disponíveis até a retenção. No entanto, as tabelas não mostram dados.
- Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro faz com que as tabelas **Utilização de Recursos e Índice do Avaliador de Carga** do novo Grupo de Entrega exibam métricas consolidadas dos Grupos de Entrega antigo e novo.

## Monitorar máquinas gerenciadas pelo Autoscale

O Autoscale é um recurso de gerenciamento de energia que permite o gerenciamento proativo de energia de todas as máquinas de SO de sessão única e multissessão registradas em um grupo de entrega. Você pode configurar o Autoscale para um grupo de entrega selecionado no Web Studio. Para obter mais informações, consulte Autoscale. Você pode monitorar as principais métricas das máquinas habilitadas para Autoscale usando o Director.

### Uso da Máquina

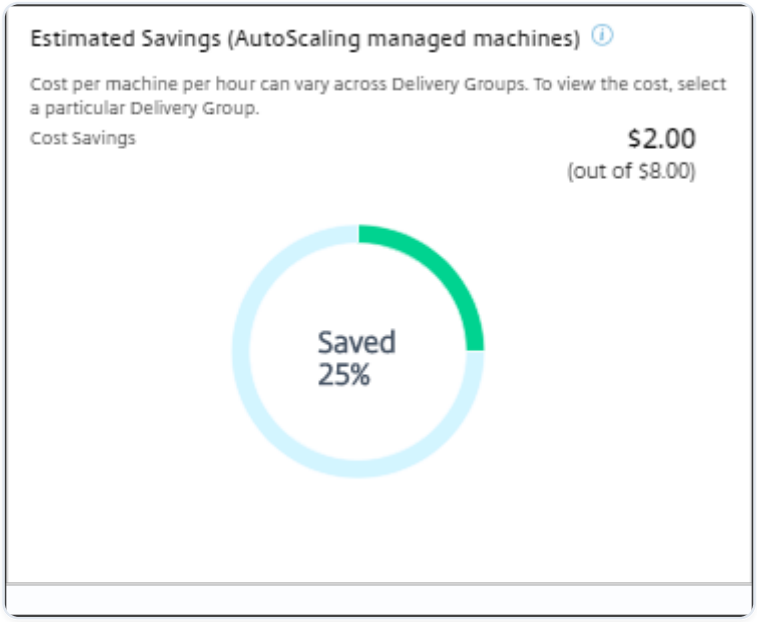
A página **Uso da Máquina** exibe o número total de máquinas de SO de sessão única e multissessão habilitadas para Autoscale que estão ligadas para um grupo de entrega e período selecionados. Essa métrica indica o uso real das máquinas no grupo de entrega. Na guia **Máquinas de SO de sessão única** ou **Máquinas de SO multissessão**, selecione o grupo de entrega e o período.

O gráfico plota as seguintes métricas:

- **Máquinas Ligadas** - o número de máquinas habilitadas para Autoscale que estão ligadas
- **Máquinas Registradas** - o número de máquinas de SO de sessão única ou multissessão registradas
- **Máquinas em Manutenção** - o número de máquinas de SO de sessão única ou multissessão com o modo de manutenção ativado

### Economia Estimada

A página **Uso da Máquina** também exibe a economia de custos estimada alcançada ao habilitar o Autoscale no grupo de entrega selecionado.




A Economia Estimada é calculada como a porcentagem de economia por máquina por hora (em US$) conforme configurado em **Editar Grupo de Entrega** > **Autoscale**. Para obter mais informações sobre como configurar a economia por máquina, consulte Autoscale.

Ao selecionar todos os grupos de entrega, o valor médio da Economia Estimada em todos os grupos de entrega é exibido.

A economia estimada ajuda os administradores a consolidar a infraestrutura existente e planejar a capacidade para alcançar o máximo de economia e utilização.

### Notificações de alerta para máquinas e sessões

O Painel do Director exibe notificações de alerta que podem ser detalhadas. Os detalhes do alerta são exibidos na página **Alertas**.

- Para criar uma política de alerta em um grupo de entrega, vá para **Alertas** > **Política de Alertas Citrix** > **Política de Grupo de Entrega**.

- Aqui, você pode definir os seguintes limites de Aviso e Crítico:
  - Máquinas com Falha (SO de sessão única) e Máquinas com Falha (SO de múltiplas sessões),
  - Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico no grupo de entrega.
- Os alertas são gerados quando a métrica correspondente no grupo de entrega atinge o limite.

Para obter mais detalhes sobre as condições da política de alerta e a criação de novas políticas de alerta, consulte Alertas e notificações.

### Status da máquina

- **Filtros** > **Máquinas** exibe o estado de energia de todas as máquinas em formato tabular. Você pode filtrar por um grupo de entrega específico.
- **Filtros** > **Sessões** exibe o filtro pelo nome da Máquina para ver as sessões associadas e seu status em tempo real.
- Em **Tendências** > **Sessões**, selecione seu grupo de entrega e período para ver a tendência das sessões e suas métricas associadas.

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

### Tendências de Avaliação de Carga

A página **Tendências** > **Índice do Avaliador de Carga** exibe um gráfico com informações detalhadas sobre a carga distribuída entre as máquinas de SO de múltiplas sessões. As opções de filtro para este gráfico incluem o grupo de entrega ou máquina de SO de múltiplas sessões em um grupo de entrega, máquina de SO de múltiplas sessões (disponível apenas se a máquina de SO de múltiplas sessões em um grupo de entrega foi selecionada) e intervalo. O Índice do Avaliador de Carga é exibido como porcentagens de CPU Total, Memória, Disco ou Sessões e é mostrado em comparação com o número de usuários conectados no último intervalo.

## Solucionar problemas de implantações

Como administrador de help desk, você pode procurar o usuário que está relatando um problema e exibir detalhes de sessões ou aplicativos associados a esse usuário. Da mesma forma, procure máquinas ou endpoints onde os problemas são relatados. Resolva problemas rapidamente monitorando as métricas relevantes e executando as ações adequadas.

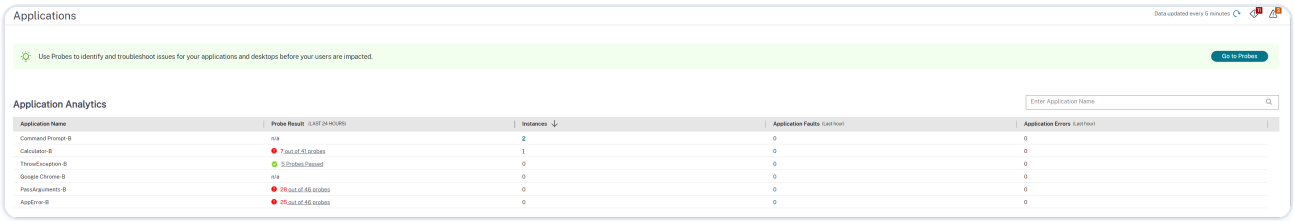
Ações disponíveis incluem:

- Encerrar um aplicativo ou processo que não responde
- Operações de sombreamento na máquina do usuário
- Fazer logoff de uma sessão que não responde
- Reiniciar a máquina
- Colocar uma máquina em modo de manutenção
- Redefinir o perfil do usuário

# Solucionar problemas de aplicativos

## Análise de Aplicativos

A exibição **Aplicativos** exibe análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho do aplicativo com eficiência. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. A exibição padrão ajuda a identificar os principais aplicativos em execução. Este recurso requer Delivery Controllers Versão 7.16 ou posterior e VDAs Versão 7.15 ou posterior.




A coluna **Resultado da Sondagem** exibe o resultado da sondagem de aplicativos executada nas últimas 24 horas. Clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** \> **Resultados da Sondagem de Aplicativos**. Para obter mais detalhes sobre como configurar sondagens de aplicativos, consulte Sondagem de Aplicativos e Desktops.

A coluna **Instâncias** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativo atualmente em execução (instâncias conectadas e desconectadas). Para solucionar problemas adicionais, clique no campo **Instâncias** para ver a página de filtros **Instâncias de Aplicativo** correspondente. Aqui, você pode selecionar instâncias de aplicativo para fazer logoff ou desconectar.

> **Nota:**
>
> Para administradores de escopo personalizado, o Director não exibe instâncias de aplicativo criadas em grupos de aplicativos. Para visualizar todas as instâncias de aplicativo, você

> deve ser um administrador completo. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX256001.

> Monitore a integridade dos aplicativos publicados em seu site com as colunas **Falhas de Aplicativo** e **Erros de Aplicativo**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao iniciar o aplicativo correspondente na última hora. Clique no campo **Falhas de Aplicativo** ou **Erros de Aplicativo** para ver os detalhes da falha na página **Tendências** \> **Falhas de Aplicativo** correspondente ao aplicativo selecionado.

As configurações da política de falha de aplicativo governam a disponibilidade e a exibição de falhas e erros. Para obter mais informações sobre as políticas e como modificá-las, consulte Políticas para monitoramento de falhas de aplicativo nas configurações de **política de monitoramento**.

### Monitoramento de aplicativos em tempo real

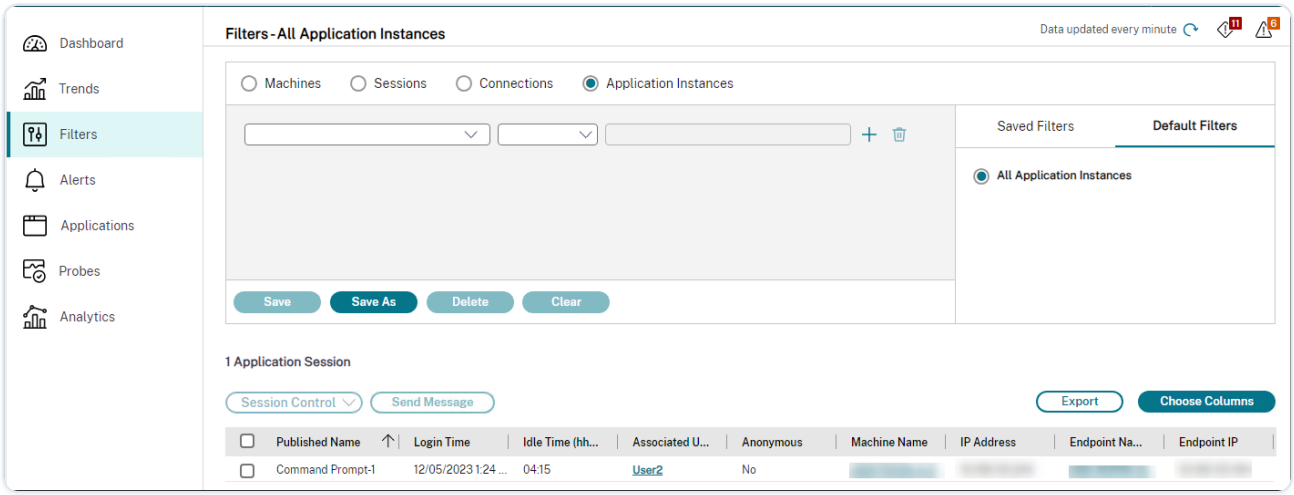
Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas baseada em aplicativos estão no setor de saúde, onde os funcionários compartilham licenças de aplicativos. Lá, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente Citrix Virtual Apps and Desktops™, reconfigurar servidores com baixo desempenho ou manter e atualizar aplicativos.

A página de filtro **Instâncias de Aplicativo** lista todas as instâncias de aplicativo em VDAs de SO de Servidor e de Sessão Única. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativo em VDAs de SO de Múltiplas Sessões que estiveram ociosas por pelo menos 10 minutos.

> **Nota:** As métricas de Instâncias de Aplicativo estão disponíveis em sites de todas as edições de licença.

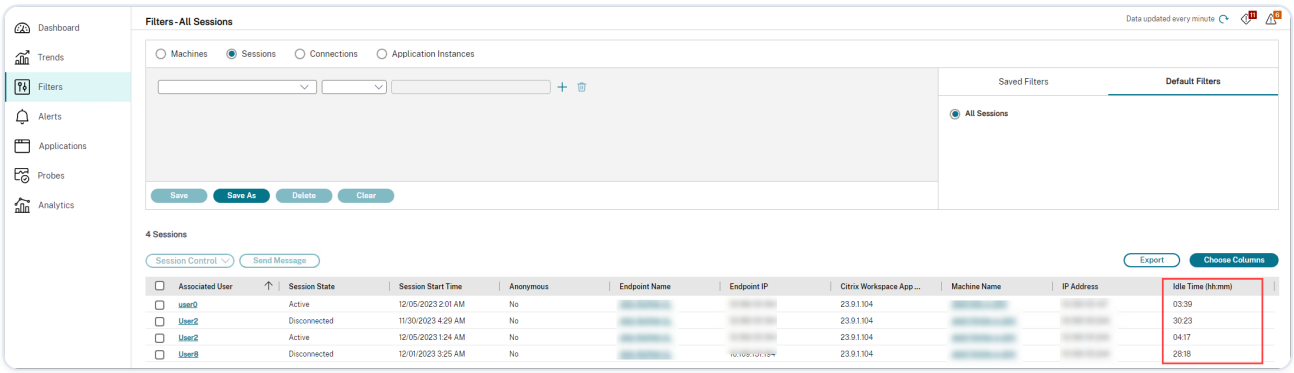
> Use essas informações para identificar as instâncias de aplicativo que estão ociosas além de um período de tempo específico e faça logoff ou desconecte-as conforme apropriado. Para fazer isso, selecione **Filtros \> Instâncias de Aplicativo** e selecione um filtro pré-salvo ou escolha **Todas as Instâncias de Aplicativo** e crie seu próprio filtro.




Um exemplo de filtro seria o seguinte. Como critérios de **Filtrar por**, escolha **Nome Publicado** (do aplicativo) e **Tempo Ocioso**. Em seguida, defina **Tempo Ocioso** como **maior ou igual a** um limite de tempo específico e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias do aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Controle de Sessão**, escolha **Logoff** ou **Desconectar** para encerrar as instâncias.

> **Nota:** Fazer logoff ou desconectar uma instância de aplicativo faz logoff ou desconecta a sessão atual, encerrando assim todas as instâncias de aplicativo que pertencem à mesma sessão.

Você pode identificar sessões ociosas na página de filtro **Sessões** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Tempo Ocioso** ou defina um filtro para identificar sessões que estão ociosas além de um limite de tempo específico. O tempo ocioso é listado para sessões em VDAs de SO multi-sessão que estiveram ociosas por pelo menos 10 minutos.




O **Tempo ocioso** é exibido como **N/A** quando a sessão ou instância do aplicativo

- não esteve ociosa por mais de 10 minutos,
- é iniciada em um VDA de SO de sessão única, ou

- é iniciada em um VDA executando a Versão 7.12 ou anterior.

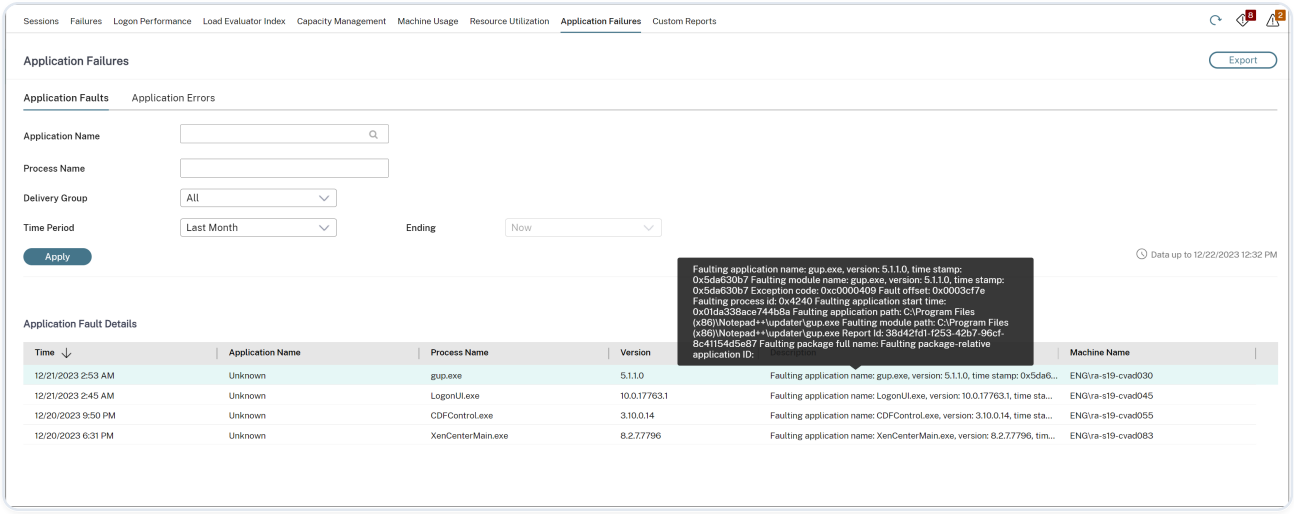
### Monitoramento histórico de falhas de aplicativo

A guia **Tendências** -\> **Falhas de Aplicativos** exibe falhas associadas aos aplicativos publicados nos VDAs.

As tendências de falha de aplicativos estão disponíveis para as últimas 2 horas, 24 horas, 7 dias e mês para sites com licença Premium e Advanced. Elas estão disponíveis para as últimas 2 horas, 24 horas e 7 dias para outros tipos de licença. As falhas de aplicativos que são registradas no Visualizador de Eventos com a origem "Application Errors" são monitoradas. Clique em **Exportar** para gerar relatórios nos formatos CSV, Excel ou PDF

As configurações de retenção de limpeza para monitoramento de falhas de aplicativo, GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays, são definidas como um dia por padrão para sites com licença Premium e não Premium. Você pode alterar essa configuração usando o comando PowerShell:

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```




As falhas são exibidas como **Falhas de Aplicativo** ou **Erros de Aplicativo** com base em sua gravidade. A guia Falhas de Aplicativo exibe falhas associadas à perda de funcionalidade ou dados. Erros de Aplicativo indicam problemas que não são imediatamente relevantes; eles significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Nome do Aplicativo Publicado**, **Nome do Processo** ou **Grupo de Entrega** e **Período de Tempo**. A tabela exibe o código da falha ou erro e uma breve descrição da falha. A descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:** O nome do aplicativo publicado é exibido como “Desconhecido” quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de desktop ou quando falha devido a uma exceção não tratada causada por um executável dependente.

> Por padrão, apenas falhas de aplicativos hospedados em VDAs de SO de várias sessões são monitoradas. Você pode modificar as configurações de monitoramento por meio das Políticas de Grupo de Monitoramento: Habilitar monitoramento de falhas de aplicativos, Habilitar monitoramento de falhas de aplicativos em VDAs de SO de sessão única e Lista de aplicativos excluídos do monitoramento de falhas. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos em Configurações de política de monitoramento.

A página **Tendências \> Resultados da Sondagem de Aplicativos** exibe os resultados da sondagem de aplicativos executada no site nas últimas 24 horas e 7 dias. Para obter mais detalhes sobre como configurar sondagens de aplicativos, consulte Sondagem de Aplicativos.

## Solucionar problemas de máquinas

> **Nota:**

> O **Citrix Health Assistant** é uma ferramenta para solucionar problemas de configuração em VDAs não registrados. A ferramenta automatiza várias verificações de integridade para identificar possíveis causas raiz para falhas de registro de VDA e problemas na inicialização da sessão e na configuração de redirecionamento de fuso horário. O artigo do Centro de Conhecimento, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém o download da ferramenta **Citrix Health Assistant** e instruções de uso.

> A exibição **Filtros > Máquinas** no console do Director exibe as máquinas configuradas no site. A guia Máquinas de SO de Múltiplas Sessões inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.

Clique na coluna **Motivo da Falha** de uma máquina com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar a falha. Os motivos da falha e as

ações recomendadas para falhas de máquina e conexão estão disponíveis em Citrix Director failure reasons and troubleshooting.

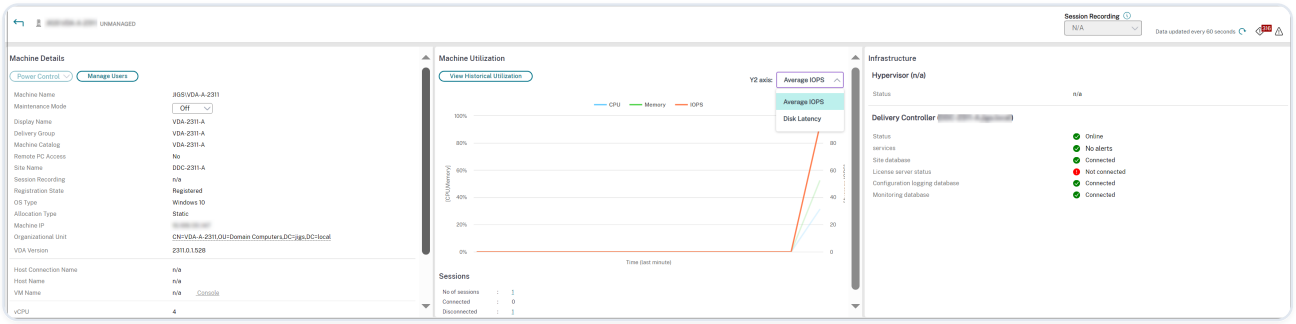
Clique no link do nome da máquina para ir para a página **Detalhes da Máquina**.

A página Detalhes da Máquina lista os detalhes da máquina, detalhes da infraestrutura e detalhes dos hotfixes aplicados na máquina.

### Utilização de recursos em tempo real baseada em máquina

O painel **Utilização da Máquina** exibe gráficos mostrando a utilização em tempo real da CPU e da memória. Além disso, gráficos de monitoramento de disco e GPU estão disponíveis para sites com Delivery Controllers e versões de VDA **7.14** ou posteriores.

Gráficos de monitoramento de disco, IOPS médio e latência de disco são medidas de desempenho importantes que ajudam a monitorar e solucionar problemas relacionados a discos VDA. O gráfico de IOPS Médio exibe o número médio de leituras e gravações em um disco. Selecione **Latência do Disco** para ver um gráfico do atraso entre uma solicitação de dados e seu retorno do disco, medido em milissegundos.




### Utilização da GPU

Selecione **Utilização da GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do Codificador e do Decodificador para solucionar problemas relacionados à GPU em VDAs de SO de múltiplas sessões e de sessão única.

**Versões de GPU suportadas:**

- GPUs NVIDIA Tesla M60 executando a versão 369.17 ou posterior do Driver de Vídeo. Para obter mais informações, consulte NVIDIA vGPU Software.
- GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12(Rome). Para obter mais informações, consulte AMD Drivers and Support.

**Drivers:**

Os drivers ou extensões apropriados devem ser instalados nos VDAs.

- Para GPUs NVIDIA, instale os drivers GRID manualmente ou via extensões. Para obter mais informações, consulte NVIDIA vGPU Software.
    - Observe que, para NVIDIA, apenas os drivers GRID são suportados. Os drivers CUDA não funcionam com a série NVadsA10 v5 e não são suportados.
    - Para um processo de exemplo para instalar drivers de GPU Nvidia Grid via extensões em máquinas baseadas no Azure, consulte NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
    - Para um processo de exemplo para instalar drivers de GPU Nvidia Grid manualmente, consulte Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Para GPUs AMD, instale os drivers gráficos AMD manualmente ou via extensões. Para obter mais informações, consulte AMD Drivers and Support.
    - Para um processo de exemplo para instalar drivers de GPU AMD via extensões em máquinas baseadas no Azure, consulte AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
    - Para um processo de exemplo para instalar drivers de GPU AMD manualmente em máquinas Azure, consulte Install AMD GPU drivers on N-series VMs running Windows.

**Notas de Uso:**

- Os gráficos de Utilização da GPU estão disponíveis apenas para VDAs executando Windows de 64 bits.
- Os VDAs devem ter o HDX 3D Pro habilitado para fornecer aceleração de GPU. Para obter mais informações, consulte GPU acceleration for Windows Single-session OS e GPU acceleration for Windows Multi-session OS.
- Quando um VDA acessa mais de uma GPU, o gráfico de utilização exibe a média das métricas de GPU coletadas das GPUs individuais. As métricas de GPU são coletadas para todo o VDA e não para processos individuais.
- Para AMD, o uso de codificador e decodificador não é suportado separadamente. Qualquer carga de trabalho de codificação/decodificação usando a GPU será relatada como a carga 3D geral no uso da GPU.
- Certifique-se de instalar o NVIDIA WMI durante a instalação. Esta janela está disponível apenas durante a instalação manual.
- Se os drivers estiverem instalados, mas o Director não detectar a GPU

    - Verifique o Gerenciador de Tarefas. Se os drivers estiverem instalados corretamente, a GPU deverá aparecer no Gerenciador de Tarefas.
    - Verifique se a máquina está registrada. Às vezes, as máquinas podem levar algum tempo para serem detectadas como online.

- Se o uso da GPU não mostrar atividade no Director, certifique-se de que a carga de trabalho que você está executando esteja usando a GPU. Para cargas de trabalho gráficas, isso pode ser ativado em Configurações > Sistema > Tela > Configurações de Gráficos > Escolher o aplicativo para definir a preferência. Certifique-se de ativar o Alto Desempenho. Às vezes, o Windows usa a CPU por padrão para cargas de trabalho gráficas quando isso é definido como padrão do sistema ou economia de energia, com base em outras configurações.
- Os dados são atualizados a cada minuto e a visualização dos dados começa dentro de um minuto após a seleção de **Utilização da GPU**.

### Utilização histórica de recursos baseada em máquina

No painel **Utilização da Máquina**, clique em **Exibir Utilização Histórica** para ver o uso histórico de recursos na máquina selecionada. Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, sessões simultâneas de pico, IOPS médio e latência de disco.

> **Nota:**
>
> A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como Permitido para coletar e exibir dados na tabela dos 10 Principais Processos na página de Utilização Histórica da Máquina. A coleta é proibida por padrão.
>
> Os dados de utilização da CPU e da memória, IOPS médio e latência de disco são coletados por padrão. Você pode desativar a coleta usando a configuração da política **Habilitar Monitoramento de Recursos**.




1. No painel **Utilização da Máquina** na exibição **Detalhes da Máquina**, selecione **Exibir Utilização Histórica**.
2. Na página **Utilização Histórica da Máquina**, defina **Período de Tempo** para visualizar o uso das últimas 2 horas, 24 horas, 7 dias, mês ou ano.

> **Nota:**
>
> Os dados de uso de IOPS médio e latência de disco estão disponíveis apenas para as últimas 24 horas, mês e ano terminando agora. Horário de término personalizado não é suportado.

3. Clique em **Aplicar** e selecione os gráficos necessários.
4. Passe o mouse sobre diferentes seções do gráfico para visualizar mais informações para o período de tempo selecionado.




Por exemplo, se você selecionar **Últimas 2 horas**, o período de linha de base é as 2 horas anteriores ao intervalo de tempo selecionado. Visualize a tendência de CPU, memória e sessão nas últimas 2 horas e no tempo de linha de base. Se você selecionar **Último mês**, o período de linha de base é o mês anterior. Selecione para visualizar a média de IOPS e a latência de disco no último mês e no tempo de linha de base.

1. Clique em **Exportar** para exportar os dados de utilização de recursos para o período selecionado. Para obter mais informações, consulte a seção Exportar relatórios em Monitorar Implantações.
2. Abaixo dos gráficos, a tabela lista os 10 principais processos com base na utilização da CPU ou da memória. Você pode classificar por qualquer uma das colunas, que mostram Nome do Aplicativo, Nome de Usuário, ID da Sessão, CPU Média, Pico de CPU, Memória Média e Pico de Memória ao longo do intervalo de tempo selecionado. As colunas IOPS e Latência de Disco não podem ser classificadas.

   > **Nota:**
   >
   > O ID da sessão para processos do sistema é exibido como "0000".

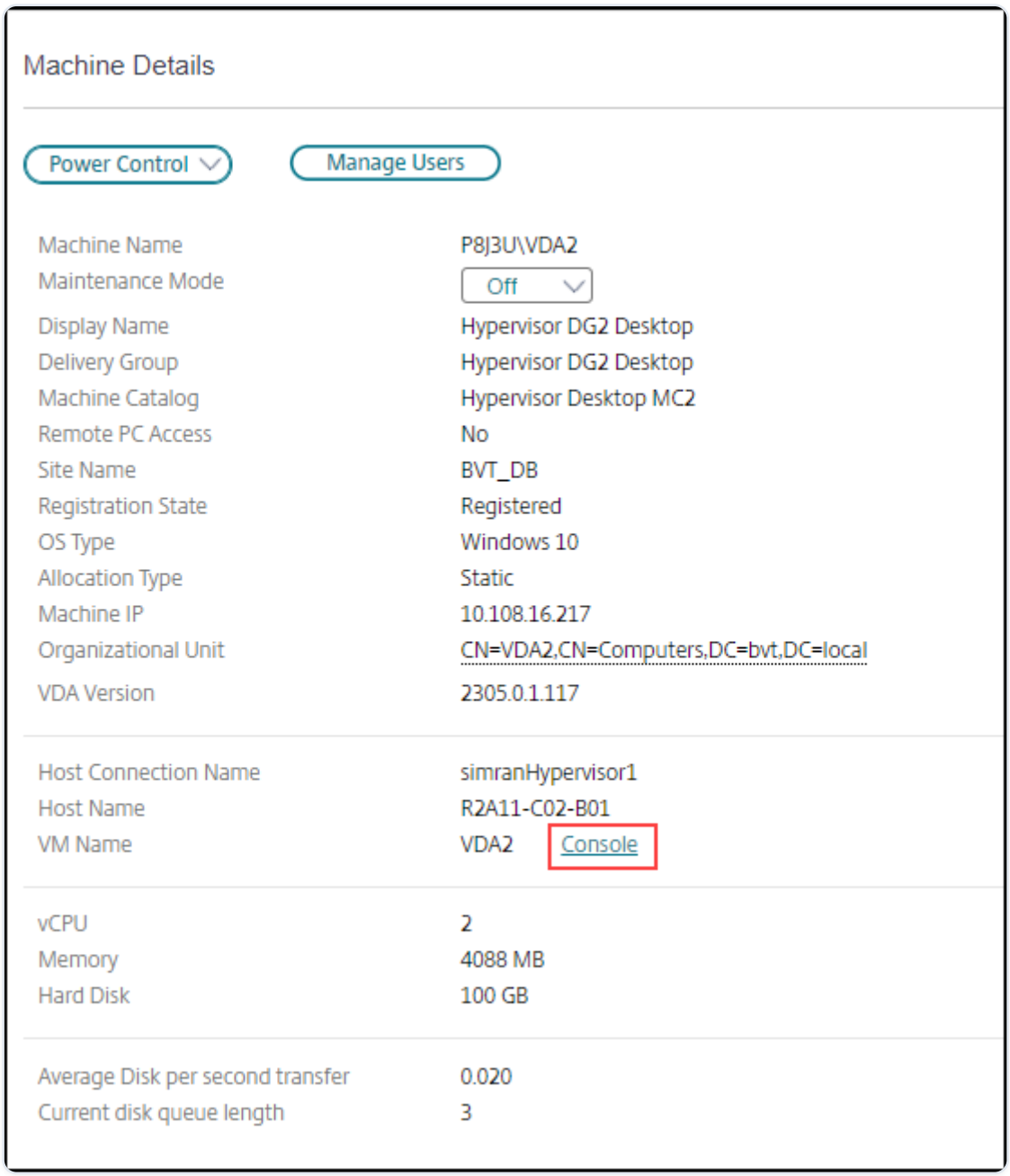
3. Para visualizar a tendência histórica do consumo de recursos de um processo específico, detalhe qualquer um dos 10 principais processos.

### Acesso ao console da máquina

Você pode acessar os consoles de máquinas de SO de sessão única e multi-sessão hospedadas no XenServer Versão 7.3 e posterior diretamente do Director. Dessa forma, você não precisa do

XenCenter para solucionar problemas em VDAs hospedados no XenServer. Para que este recurso esteja disponível:

- É necessário o Delivery Controller Versão 7.16 ou posterior.
- O XenServer que hospeda a máquina deve ser da Versão 7.3 ou posterior e deve ser acessível a partir da interface do usuário do Director.



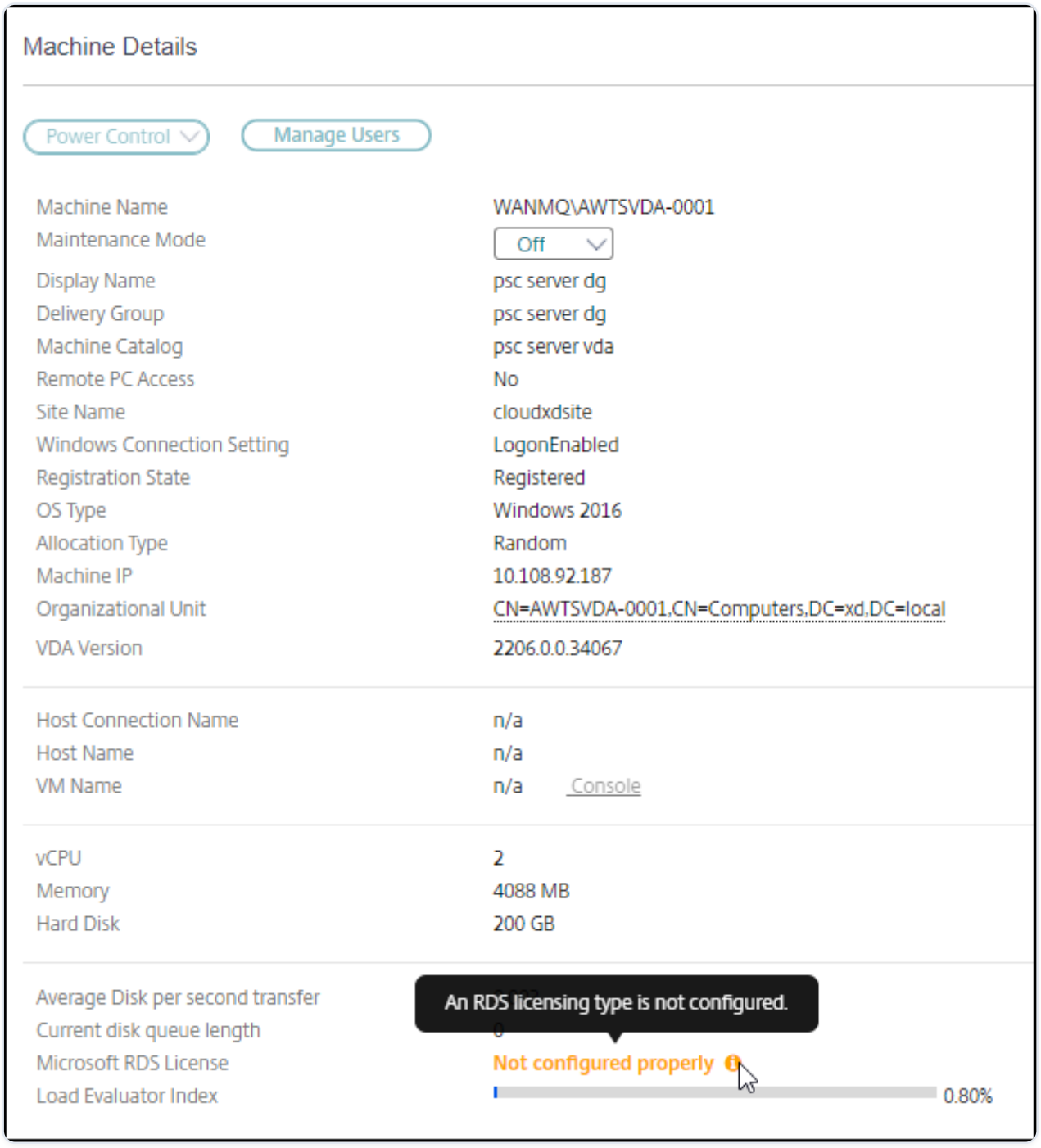

Para solucionar problemas em uma máquina, clique no link **Console** no painel Detalhes da Máquina correspondente. Após a autenticação das credenciais do host que você fornece, o console da máquina é aberto em uma nova guia usando noVNC, um cliente VNC baseado na web. Agora você tem acesso ao console com teclado e mouse.

**Nota:**

- Este recurso não é compatível com o Internet Explorer 11.
- Se o ponteiro do mouse no console da máquina estiver desalinhado, consulte CTX230727 para obter as etapas para corrigir o problema.
- O Director inicia o acesso ao console em uma nova guia, certifique-se de que as configurações do seu navegador permitam pop-ups.
- Por motivos de segurança, a Citrix® recomenda que você instale certificados SSL em seu navegador.

### Integridade da licença RDS da Microsoft

Você pode visualizar o status da licença RDS da Microsoft no painel Detalhes da Máquina nas páginas **Detalhes da Máquina** e **Detalhes do Usuário** para máquinas de SO de múltiplas sessões.




Uma das seguintes mensagens é exibida:

- Licença disponível
- Não configurado corretamente (aviso)
- Erro de licença (erro)
- Versão VDA incompatível (erro)

**Nota:**

O status de integridade da licença Microsoft RDS para máquinas em período de carência com licença válida exibe uma mensagem de **Licença disponível** em verde. Renove sua licença antes que ela expire.

Para mensagens de aviso e erro, passe o mouse sobre o ícone de informações para visualizar informações adicionais, conforme mostrado na tabela a seguir.

| TIPO DE MENSAGEM | MENSAGENS NO DIRECTOR |
|---|---|
| Erro | Disponível para VDAs versão 7.16 e posterior. |
| Erro | Novas conexões RDS não são permitidas. |
| Erro | A licença RDS da Microsoft excedeu seu período de carência. |
| Erro | Um Servidor de Licenças não está configurado para o nível de SO exigido com o tipo de licenciamento de Acesso de Cliente por Dispositivo. |
| Erro | O Servidor de Licenças configurado é incompatível com o nível de SO do Host RDS com o tipo de licenciamento de Acesso de Cliente por Dispositivo. |
| Aviso | O Servidor de Terminal Pessoal não é um tipo de licenciamento RDS válido em uma implantação do Citrix Virtual Apps and Desktops™. |
| Aviso | A Área de Trabalho Remota para Administração não é um tipo de licenciamento válido em uma implantação do Citrix Virtual Apps and Desktops. |
| Aviso | Um tipo de licenciamento RDS não está configurado. |
| Aviso | O Controlador de Domínio ou Servidor de Licenças está inacessível com o tipo de |

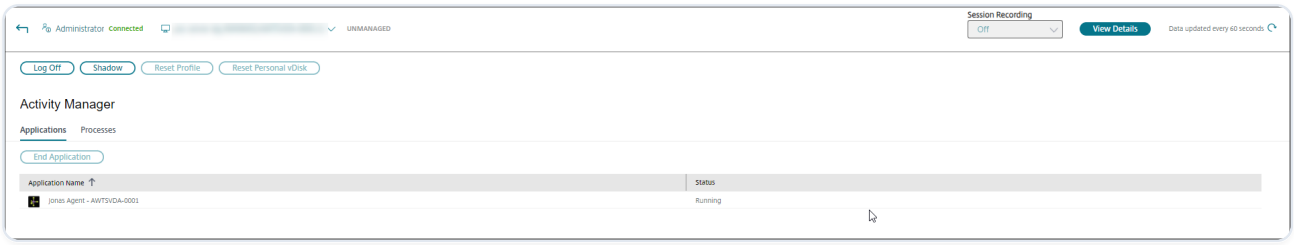
| TIPO DE MENSAGEM | MENSAGENS NO DIRECTOR |
| --- | --- |
| | licenciamento RDS de Acesso de Cliente por Usuário. |
| Aviso | Com o tipo de licenciamento de Acesso de Cliente por Dispositivo, a licença do Dispositivo Cliente não pode ser determinada, pois o servidor de licenças para o nível de SO exigido está inacessível. |

**Nota:**

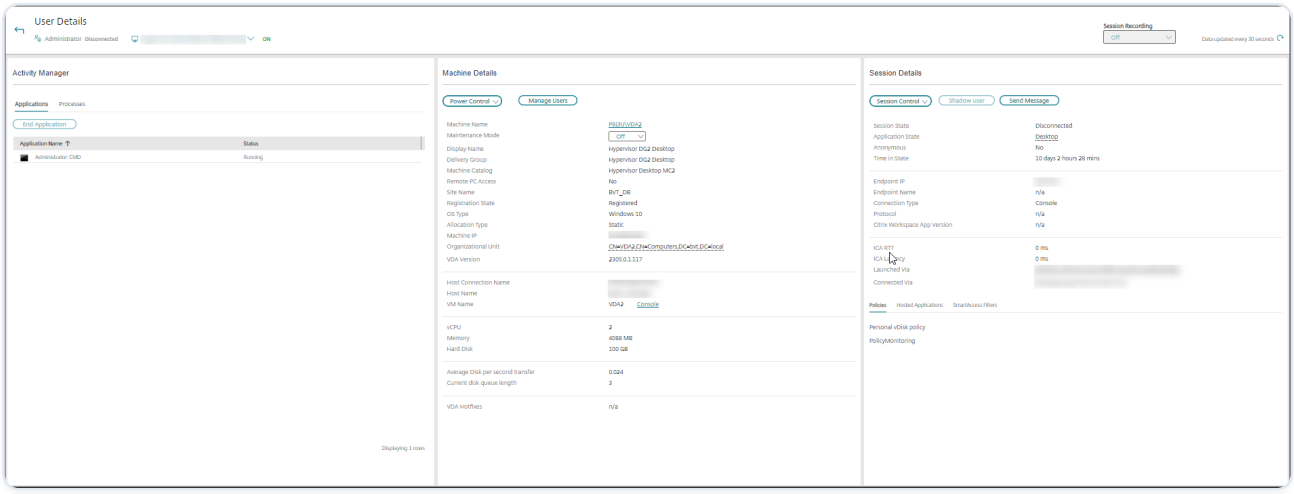
Este recurso é aplicável apenas para CAL RDS da Microsoft (Licença de Acesso de Cliente).

## Solucionar problemas do usuário

Use a exibição **Help Desk** do Director (página **Activity Manager**) para visualizar informações sobre o usuário ou a sessão:




Clicar em **View Details** no Activity Manager para um usuário abre a página **User Details**. Clicar em **View Details** no Activity Manager para um endpoint abre a página **Endpoint Details**.



### Seletor de Sessão

Se o usuário iniciou várias sessões, o seletor de sessão ajuda a selecionar uma sessão.




Escolha uma sessão para visualizar os detalhes.

- Verifique os detalhes sobre a sessão, a experiência de login do usuário, a inicialização da sessão, a conexão e os aplicativos.
- você pode fazer Shadow na máquina do usuário.
- Grave a sessão ICA®.

### Status de otimização do Microsoft Teams

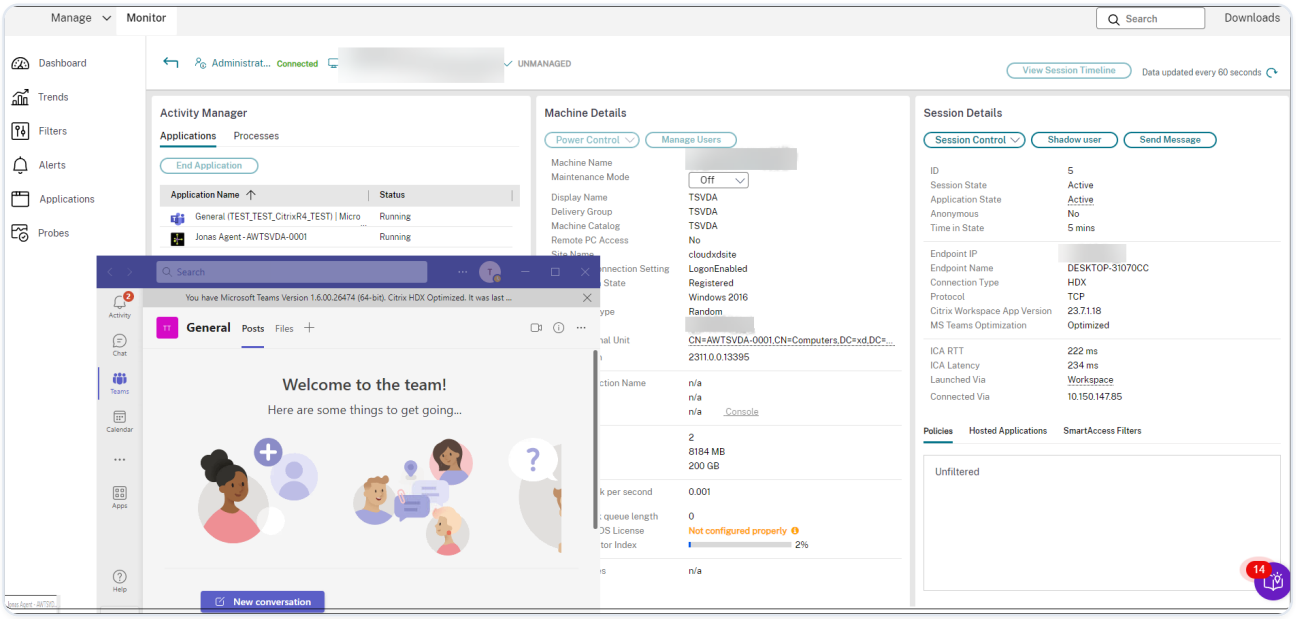
O Director exibe o status de otimização do Microsoft Teams para sessões HDX™ na página **User Details** > painel **Session Details** > campo **MS Teams Optimization**. O Microsoft Teams otimizado é fundamental para uma melhor experiência do usuário, como áudio e vídeo nítidos. A visibilidade do status de otimização do Microsoft Teams é útil para reduzir o tempo necessário para resolver tickets e ajuda os administradores a identificar métricas importantes durante a solução de problemas.

> **Nota:**

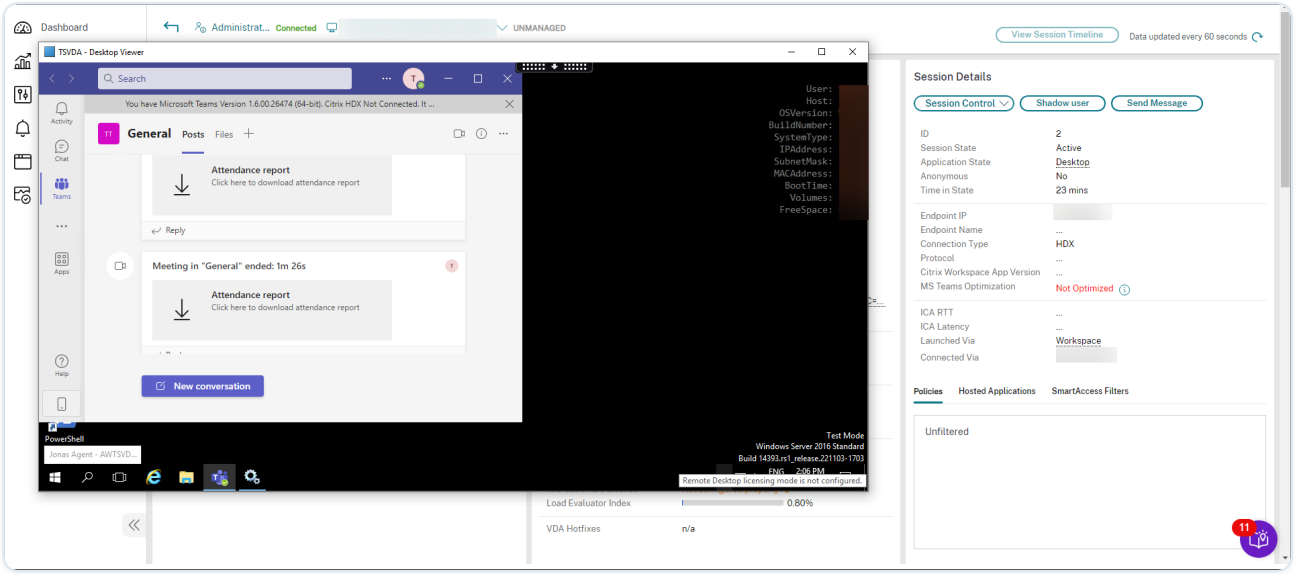
> O Citrix Director oferece suporte ao Microsoft Teams versão 2.1 ou anterior.

> Pré-requisitos:

- Os VDAs estão executando a versão 2311 e posterior.
- As versões do aplicativo Citrix Workspace compatíveis estão listadas em Otimização para Microsoft Teams.
- O Microsoft Teams é executado como um aplicativo publicado ou dentro de um desktop publicado.
- Serviços cruciais, como o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX, estão em execução.




Se o Microsoft Teams não estiver otimizado, a dica de ferramenta fornece um link para um artigo de solução de problemas externo ao vivo do HDX contendo dicas para otimizar o Microsoft Teams. Solução de problemas de otimização HDX.



### Dicas de solução de problemas

Solucione o problema com as ações recomendadas na tabela a seguir e, se necessário, encaminhe o problema ao administrador apropriado.

| PROBLEMA DO USUÁRIO | SUGESTÕES |
|---|---|
| O logon demora muito ou falha intermitentemente ou repetidamente | Diagnosticar problemas de logon do usuário |
| A inicialização da sessão demora muito ou falha intermitentemente ou repetidamente | Diagnosticar problemas de inicialização da sessão |
| A resposta da sessão está lenta ou não responde | Diagnosticar problemas de desempenho da sessão |
| Aplicativo está lento ou não responde | Resolver falhas de aplicativo |
| Conexão falhou | Restaurar conexões de desktop |
| Sessão está lenta ou não responde | Restaurar sessões |
| Gravar sessões | Gravar sessões |
| Vídeo está lento ou com baixa qualidade | Executar relatórios do sistema de canal HDX |

> **Nota:** Para garantir que a máquina não esteja em modo de manutenção, na exibição Detalhes do Usuário, revise o painel Detalhes da Máquina.

### Logon da Sessão

A exibição **Detalhes do Usuário** > guia **Logon da Sessão** exibe uma visão abrangente do processo de logon da sessão. A guia contém o gráfico de fases de Duração do Logon com as várias fases de logon plotadas. Use esses dados para solucionar problemas de logon do usuário. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

### Desempenho da Sessão

A guia **Desempenho da Sessão** possui fluxos de trabalho de solução de problemas aprimorados, começando com a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. O painel **Topologia da Sessão** fornece uma representação visual do caminho em sessão para sessões HDX conectadas. O painel **Métricas**

**de Desempenho** fornece tendências para as métricas de sessão como ICARTT, Latência ICA, Quadros Por Segundo, Largura de Banda de Saída Disponível e Largura de Banda de Saída Consumida, ajudando a indicar como essas métricas se comportaram ao longo do tempo. Para obter mais informações, consulte Diagnosticar problemas de desempenho da sessão.

### Dicas de pesquisa

Quando você digita o nome do usuário em um campo de Pesquisa, o Director pesquisa usuários no Active Directory em todos os sites configurados para oferecer suporte ao Director.

Quando você digita o nome de uma máquina multiusuário em um campo de Pesquisa, o Director exibe os Detalhes da Máquina para a máquina especificada.

Quando você digita um nome de endpoint em um campo de Pesquisa, o Director usa as sessões não autenticadas (anônimas) e autenticadas que estão conectadas a um endpoint específico. Essa pesquisa permite solucionar problemas de sessões não autenticadas. Certifique-se de que os nomes dos endpoints sejam exclusivos para permitir a solução de problemas de sessões não autenticadas.

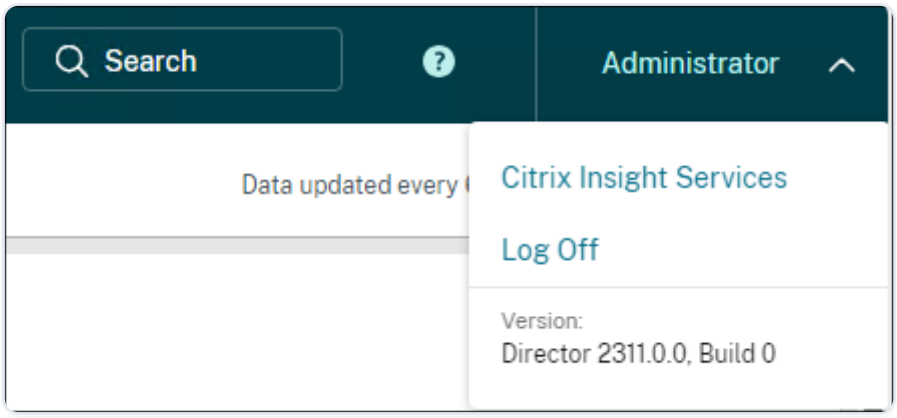
Os resultados da pesquisa também incluem usuários que não estão usando ou não estão atribuídos a uma máquina no momento.

- As pesquisas não diferenciam maiúsculas de minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome composto, separado por um espaço, os resultados incluem correspondências para ambas as strings. Os exemplos de nomes compostos são nome de usuário, sobrenome e primeiro nome, ou nome de exibição. Por exemplo, se você digitar jo rob, os resultados podem incluir strings como “John Robertson” ou "Robert Jones".

Para retornar à página inicial, clique no **logotipo do Director**.

### Acessar o Citrix Insight Services

Você pode acessar o Citrix Insight Services (CIS) na lista suspensa **Usuário** no Director para acessar insights de diagnóstico adicionais. Os dados disponíveis no CIS vêm de fontes como Call Home e Citrix Scout.




### Carregar informações de solução de problemas para o Suporte Técnico da Citrix

Execute o Citrix Scout a partir de um único Delivery Controller™ ou VDA para capturar pontos de dados importantes e rastreamentos do Citrix Diagnostics Facility (CDF) para solucionar problemas em computadores selecionados. O Scout oferece a capacidade de carregar os dados com segurança para a plataforma CIS para auxiliar o Suporte Técnico da Citrix na solução de problemas. O Suporte Técnico da Citrix usa a plataforma CIS para reduzir o tempo de resolução de problemas relatados pelos clientes.

O Scout é instalado com os componentes do Citrix Virtual Apps and Desktops™. Dependendo da versão do Windows, o Scout aparece no menu **Iniciar do Windows** ou na Tela Inicial quando você instala ou atualiza para o Citrix Virtual Apps and Desktops.

Para iniciar o Scout, no menu Iniciar ou na tela Iniciar, selecione **Citrix \> Citrix Scout**.

Para obter informações sobre como usar e configurar o Scout, e para um FAQ, consulte CTX130147.

## Diagnosticar problemas de inicialização de sessão

Além das fases do processo de logon mencionadas na seção Diagnosticar problemas de logon do usuário, o Director exibe a duração da inicialização da sessão. Isso é dividido em Duração da Inicialização da Sessão do Workspace App e Duração da Inicialização da Sessão do VDA nas páginas **Detalhes do Usuário** e **Detalhes da Máquina**. Essas duas durações contêm ainda fases individuais cujas durações de inicialização também são exibidas. Esses dados ajudam você a entender e solucionar problemas de alta duração de inicialização da sessão. Além disso, a duração de cada fase envolvida na inicialização da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de Mapeamento de Unidade for alto, você pode verificar se todas as unidades válidas estão mapeadas corretamente na GPO ou no script. Este recurso está disponível no Delivery Controller versão 7 1906 e posterior e VDAs 1903 e posterior.

### Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração da inicialização da sessão sejam exibidos:

- Delivery Controller™ 7 1906 ou posterior.
- VDA 1903 ou posterior.
- O serviço Citrix End User Experience Monitoring (EUEM) deve estar em execução no VDA.

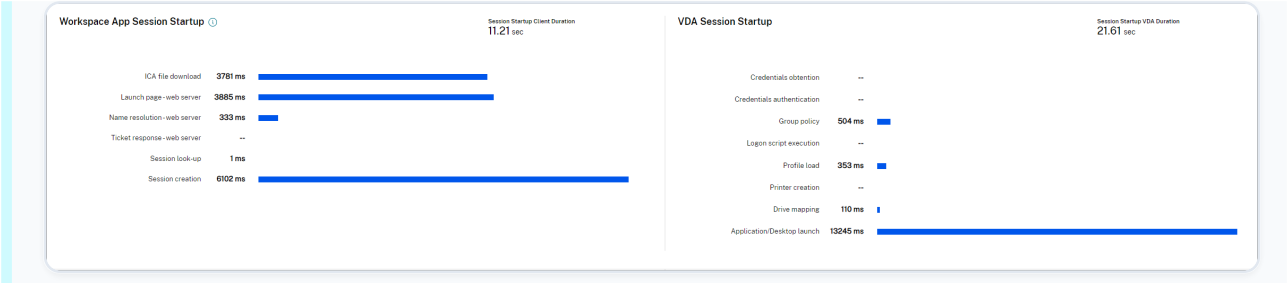
### Limitações

As seguintes limitações se aplicam quando o Director exibe os dados de duração da inicialização da sessão.

- A duração da inicialização da sessão está disponível apenas para sessões HDX™.
- Para inicializações de sessão de iOS e Android OS, apenas a Duração de Inicialização do VDA está disponível.
- A Duração de Download de Arquivo ICA® (IFDCD) está disponível apenas quando o Workspace App é detectado ao iniciar a partir de um navegador.
- Para inicializações de sessão de Mac OS, o IFDCD está disponível apenas para o Workspace App 1902 ou posterior.
- Para inicializações de sessão de Windows OS, o IFDCD está disponível para o Workspace app 1902 e posterior. Para versões anteriores, o IFDCD é exibido apenas para inicializações de aplicativos a partir do navegador com o Workspace app detectado.

**Notas:**

- Se você enfrentar problemas na exibição da duração da inicialização das sessões após o cumprimento dos pré-requisitos, visualize os logs do servidor Director e do VDA conforme descrito em CTX130320. Para sessões compartilhadas (vários aplicativos iniciados na mesma sessão), as métricas de Inicialização do Workspace App são exibidas para a conexão mais recente ou o lançamento de aplicativo mais recente.
- Algumas métricas na Inicialização da Sessão do VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.




## Fases de inicialização da sessão do Workspace App

### DURAÇÃO DE INICIALIZAÇÃO DA SESSÃO DO CLIENTE (SSCD)

Quando essa métrica é alta, indica um problema do lado do cliente que está causando longos tempos de inicialização. Revise as métricas subsequentes para determinar a provável causa raiz do problema. O SSCD começa o mais próximo possível do momento da solicitação (clique do mouse). Ele termina quando a conexão ICA entre o dispositivo cliente e o VDA é estabelecida. No caso de uma sessão compartilhada, essa duração é muito menor, pois muitos dos custos de configuração associados à criação de uma nova conexão com o servidor não são incorridos. No nível seguinte, há várias métricas detalhadas disponíveis.

### DURAÇÃO DO DOWNLOAD DO ARQUIVO ICA

Este é o tempo que o cliente leva para baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou desktop) no Workspace Application.
2. Uma solicitação do usuário é enviada ao StoreFront™ através do Citrix Gateway (se configurado), que envia a solicitação ao Delivery Controller.
3. O Delivery Controller encontra uma máquina disponível para a solicitação e envia as informações da máquina e outros detalhes para o StoreFront. Além disso, o StoreFront solicita e recebe um tíquete único da Secure Ticket Authority.
4. O StoreFront gera um arquivo ICA e o envia ao usuário via Citrix Gateway (se configurado).

IFDCD representa o tempo que leva para o processo completo (etapas 1–4). A duração do IFDCD para de contar quando o cliente recebe o arquivo ICA.

LPWD é o componente StoreFront do processo.

Se o IFDCD for alto (mas o LPWD for normal), o processamento do lançamento no lado do servidor foi bem-sucedido, mas houve problemas de comunicação entre o dispositivo cliente e o StoreFront. Isso resulta de problemas de rede entre as duas máquinas. Portanto, você pode solucionar possíveis problemas de rede primeiro.

### DURAÇÃO DO SERVIDOR WEB DA PÁGINA DE LANÇAMENTO (LPWD)

Este é o tempo levado para processar a página de lançamento (launch.aspx) no StoreFront. Se o LPWD for alto, pode haver um gargalo no StoreFront.

As possíveis causas incluem:

- Carga alta no StoreFront. Tente identificar a causa da lentidão verificando os logs do Internet Information Services (IIS) e ferramentas de monitoramento, Gerenciador de Tarefas, Monitor de Desempenho e assim por diante.
- O StoreFront está com problemas para se comunicar com outros componentes, como o Delivery Controller. Verifique se a conexão de rede entre o StoreFront e o Delivery Controller está lenta ou se alguns Delivery Controllers estão inativos ou sobrecarregados.

### DURAÇÃO DO SERVIDOR WEB DE RESOLUÇÃO DE NOMES (NRWD)

Este é o tempo que o Delivery Controller leva para resolver o nome de um aplicativo/desktop publicado para um endereço IP de máquina VDA.

Quando essa métrica é alta, indica que o Delivery Controller está demorando muito para resolver o nome de um aplicativo publicado para um endereço IP.

As possíveis causas incluem um problema no cliente, problemas com o Delivery Controller, como o Delivery Controller estar sobrecarregado, ou um problema com o link de rede entre eles.

### DURAÇÃO DO SERVIDOR WEB DE RESPOSTA DE TICKET (TRWD)

Esta duração indica o tempo que leva para obter um ticket (se necessário) do Servidor Secure Ticket Authority (STA) ou do Delivery Controller. Quando essa duração é alta, indica que o servidor STA ou o Delivery Controller estão sobrecarregados.

### DURAÇÃO DO CLIENTE DE PESQUISA DE SESSÃO (SLCD)

Esta duração representa o tempo levado para consultar cada sessão para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode manipular a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

### DURAÇÃO DO CLIENTE DE CRIAÇÃO DE SESSÃO (SCCD)

Esta duração representa o tempo levado para criar uma sessão, desde o momento em que wfica32.exe (ou um arquivo equivalente similar) é iniciado até o momento em que a conexão é estabelecida.

## Fases de inicialização da sessão VDA

### DURAÇÃO DE INICIALIZAÇÃO DA SESSÃO VDA (SSVD)

Esta duração é a métrica de alto nível de inicialização de conexão do lado do servidor que engloba o tempo que o VDA leva para realizar toda a operação de inicialização. Quando essa métrica é alta, indica que há um problema no VDA que aumenta os tempos de inicialização da sessão. Isso inclui o tempo gasto no VDA realizando toda a operação de inicialização.

### DURAÇÃO DA OBTENÇÃO DE CREDENCIAIS DO VDA (COVD)

O tempo que o VDA leva para obter as credenciais do usuário.

Essa duração pode aumentar artificialmente se um usuário não fornecer as credenciais em tempo hábil. Portanto, não está incluída na Duração de Inicialização do VDA. Esse tempo provavelmente será significativo apenas se o login manual estiver sendo usado e a caixa de diálogo de credenciais do lado do servidor for exibida (ou se um aviso legal for exibido antes do início do login).

### DURAÇÃO DA AUTENTICAÇÃO DE CREDENCIAIS DO VDA (CAVD)

Este é o tempo que o VDA leva para autenticar as credenciais do usuário contra o provedor de autenticação. Eles podem ser Kerberos, Active Directory ou uma Interface de Provedor de Suporte de Segurança (SSPI).

### DURAÇÃO DA POLÍTICA DE GRUPO DO VDA (GPVD)

Essa duração é o tempo levado para aplicar objetos de política de grupo durante o logon.

### DURAÇÃO DA EXECUÇÃO DE SCRIPT DE LOGON DO VDA (LSVD)

Este é o tempo que o VDA leva para executar os scripts de logon do usuário.

Considere tornar assíncronos os scripts de logon do usuário ou do grupo. Considere otimizar quaisquer scripts de compatibilidade de aplicativos ou usar variáveis de ambiente em vez disso.

### DURAÇÃO DO CARREGAMENTO DE PERFIL DO VDA (PLVD)

Este é o tempo que o VDA leva para carregar o perfil do usuário.

Se essa duração for alta, considere sua configuração de Perfil de Usuário. O tamanho e a localização do perfil móvel contribuem para inícios de sessão lentos. Quando um usuário faz logon em uma sessão onde perfis móveis e pastas pessoais do Terminal Services estão habilitados, o conteúdo do perfil móvel e o acesso a essa pasta são mapeados durante o logon. Isso consome recursos extras. Às vezes, isso pode consumir uma quantidade significativa do uso da CPU. Considere usar as pastas **Terminal Services home** com pastas pessoais redirecionadas para mitigar esse problema. Em geral, considere usar o Citrix Profile Management para gerenciar perfis

de usuário em ambientes Citrix. Se você estiver usando o Citrix Profile Management e tiver tempos de logon lentos, verifique se o seu software antivírus está bloqueando a ferramenta Citrix Profile Management.

### DURAÇÃO DA CRIAÇÃO DE IMPRESSORA DO VDA (PCVD)

Este é o tempo que o VDA leva para mapear as impressoras cliente do usuário de forma síncrona. Se a configuração estiver definida para que a criação da impressora seja realizada de forma assíncrona, o valor não é registrado para PCVD, pois não afeta a conclusão da inicialização da sessão.

O tempo excessivo gasto no mapeamento de impressoras é frequentemente o resultado das configurações da política de criação automática de impressoras. O número de impressoras adicionadas localmente nos dispositivos cliente dos usuários e sua configuração de impressão podem afetar diretamente os tempos de início da sessão. Quando uma sessão é iniciada, o Citrix Virtual Apps and Desktops™ precisa criar cada impressora mapeada localmente no dispositivo cliente. Considere reconfigurar suas políticas de impressão para reduzir o número de impressoras que são criadas, especialmente quando os usuários têm muitas impressoras locais. Para fazer isso, edite a política de criação automática de impressoras no Delivery Controller e no Citrix Virtual Apps and Desktops.

### DURAÇÃO DO VDA DE MAPEAMENTO DE UNIDADE (DMVD)

Este é o tempo levado pelo VDA para mapear as unidades cliente, dispositivos e portas do usuário.

Certifique-se de que suas políticas base incluam configurações para desabilitar canais virtuais não utilizados. Por exemplo, mapeamento de áudio ou porta COM, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

### DURAÇÃO DO VDA DE INICIALIZAÇÃO DE APLICATIVO/ÁREA DE TRABALHO (ALVD/DLVD)

Esta fase é uma combinação da duração do Userinit e do Shell. Quando um usuário faz logon em uma máquina Windows, o winlogon executa o userinit.exe. O Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe. Userinit representa a duração entre o início do userinit.exe e o início da interface do usuário para a área de trabalho virtual ou aplicativo. A duração do Shell é o tempo entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

### DURAÇÃO DO VDA DE CRIAÇÃO DE SESSÃO (SCVD)

Este tempo inclui qualquer atraso diverso no tempo de criação da sessão no VDA.

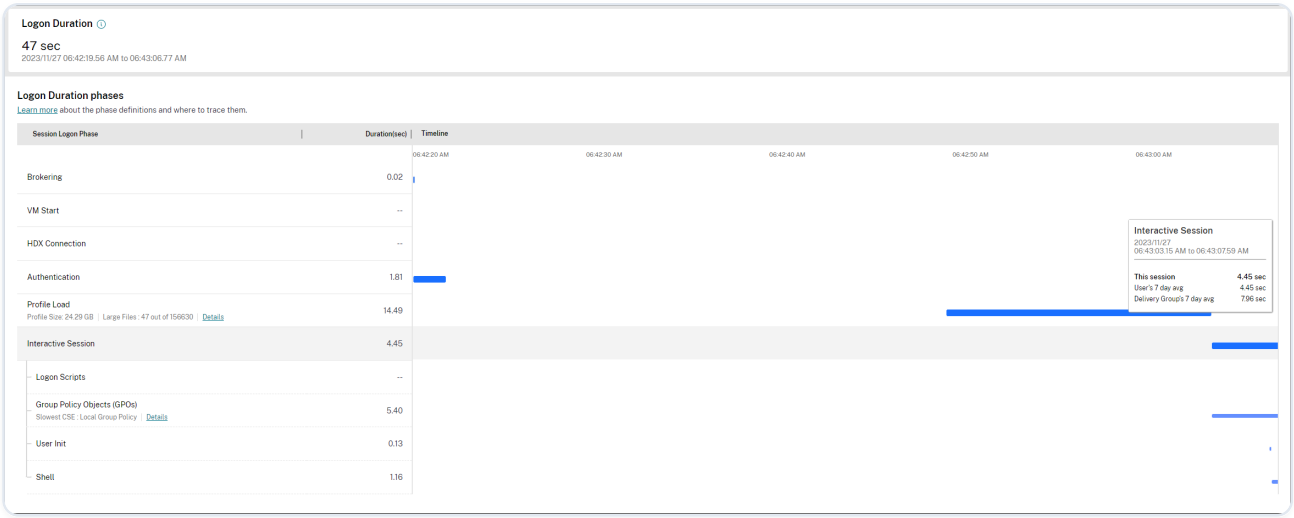
## Diagnosticar problemas de logon do usuário

A guia **Detalhes do Usuário** > **Logon da Sessão** exibe uma visão abrangente do processo de logon da sessão. Use esses dados para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a um desktop ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o Protocolo de Área de Trabalho Remota ou reconectar-se de sessões desconectadas. Especificamente, a duração do logon não é medida quando um usuário se conecta inicialmente usando um protocolo não-HDX e se reconecta usando HDX.

À medida que os usuários fazem logon no Citrix Virtual Apps and Desktops™, o Serviço de Monitoramento rastreia as fases do processo de logon. As fases começam desde o momento em que o usuário se conecta do aplicativo Citrix Workspace™ até o momento em que o aplicativo ou desktop está pronto para uso.

A guia **Logon da Sessão** contém o gráfico de fases de Duração do Logon com as várias fases de logon plotadas. A Duração do Logon representa o tempo gasto para estabelecer a conexão e obter um aplicativo ou desktop do Delivery Controller™ e o tempo gasto para autenticar e fazer logon em um aplicativo ou desktop virtual. As informações de duração são apresentadas em segundos (ou frações de segundos).




O gráfico de fases de Duração do Logon fornece uma visão clara das diferentes fases de logon e seus tempos de início e término. O gráfico mostra a sobreposição das fases de logon individuais. O tempo total de logon pode não ser a soma das durações das fases de logon individuais. Isso ocorre porque as fases individuais podem se sobrepor e nem todas as fases de logon fazem parte desta representação. Além disso, certas fases podem se estender mesmo depois que o usuário começa a interagir com o aplicativo ou desktop virtual, e essa duração não é medida como parte da duração geral do logon.

Use esta exibição para identificar fases de logon específicas que causam um atraso no lançamento da sessão. A definição para cada fase de logon e a fonte do evento de onde você pode rastrear informações ajudam na solução de problemas. Passar o mouse sobre o gráfico exibe uma dica de ferramenta contendo a duração da fase para a sessão atual, bem como a média de 7 dias do usuário e a média de 7 dias do grupo de entrega. Essas informações ajudam a comparar a duração do logon da sessão atual com os valores médios de 7 dias. Você pode detalhar ainda mais as medições de subfase no caso de GPO e Detalhes do Perfil. Essa visualização ajuda a entender e solucionar problemas relacionados à duração do logon facilmente.

### Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração do logon e os detalhamentos apareçam:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Serviço de Gerenciamento de Perfil do Citrix esteja em execução.
3. Para sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Não processar a lista de execução herdada**.
4. O rastreamento de processo de auditoria deve ser habilitado para o detalhamento da Sessão Interativa.
5. Para o detalhamento de GPO, aumente o tamanho dos logs operacionais da Política de Grupo.

> **Notas:**
>
> - A duração do logon é suportada apenas no shell padrão do Windows (explorer.exe) e não em shells personalizados.
> - A duração do logon para o Acesso Remoto a PC está disponível apenas quando o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** são instalados como componentes extras durante a instalação do Acesso Remoto a PC. Para obter mais informações, consulte a Etapa 4 em Considerações sobre configuração e sequência do Acesso Remoto a PC.

### Etapas para solucionar problemas de logon de usuário

1. Na exibição **Detalhes do Usuário** > guia **Logon da Sessão**, solucione o estado do logon usando o gráfico de Duração do Logon.

- Se o usuário estiver fazendo logon, a exibição reflete o processo de logon.
- Se o usuário estiver logado, o painel Duração do Logon exibe o tempo que o usuário levou para fazer logon na sessão atual.

2. Examine as fases do processo de logon.

**Fases do processo de logon**

#### INTERMEDIAÇÃO

Tempo levado para decidir qual desktop atribuir ao usuário.

#### INICIALIZAÇÃO DA VM

Se a sessão exigir a inicialização de uma máquina, a inicialização da VM é o tempo necessário para iniciar a máquina virtual.

#### CONEXÃO HDX

Tempo levado para concluir as etapas necessárias para configurar a conexão HDX do cliente para a máquina virtual.

#### AUTENTICAÇÃO

Tempo levado para concluir a autenticação na sessão remota.

#### GPOS

Se as configurações de Política de Grupo estiverem habilitadas nas máquinas virtuais, este é o tempo necessário para aplicar os objetos de política de grupo durante o logon. O detalhamento do tempo necessário para aplicar cada política de acordo com as CSEs (Extensão do Lado do Cliente) está disponível como uma dica de ferramenta ao passar o mouse sobre a barra GPO.




Clique em **Detalhes** para ver uma tabela com o status da política e o nome GPO correspondente. As durações de tempo no detalhamento representam apenas o tempo de processamento do CSE

e não somam o tempo total do GPO. Você pode copiar a tabela de detalhamento para solução de problemas adicionais ou uso em relatórios. O tempo GPO para as políticas é recuperado dos logs do Visualizador de Eventos. Os logs podem ser sobrescritos dependendo da memória alocada para os logs operacionais (o tamanho padrão é 4 MB). Para obter mais informações sobre como aumentar o tamanho do log para os logs operacionais, consulte o artigo do Microsoft TechNet Configuring the Event Logs.

### SCRIPTS DE LOGON

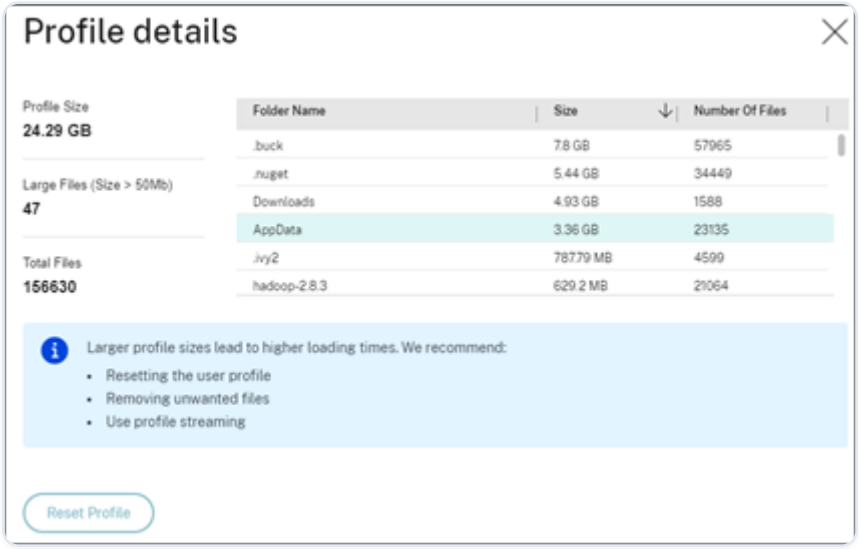
Se os scripts de logon estiverem configurados para a sessão, este é o tempo levado para que os scripts de logon sejam executados.

### CARREGAMENTO DE PERFIL

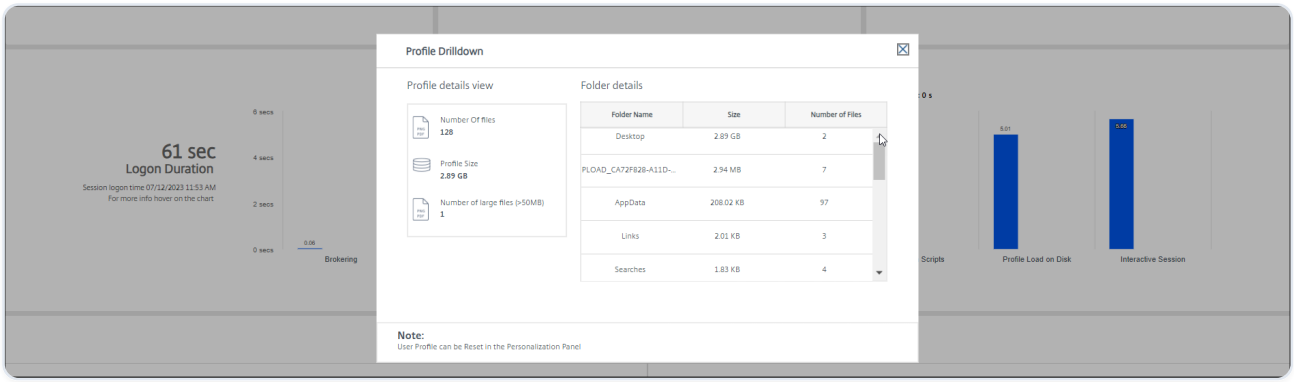
Se as configurações de perfil estiverem configuradas para o usuário ou a máquina virtual, este é o tempo necessário para o perfil carregar.

Se o Citrix Profile Management estiver configurado, a barra de Carregamento de Perfil incluirá o tempo gasto pelo Citrix Profile Management para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management está configurado, a barra de Carregamento de Perfil exibe uma duração aumentada. Esse aumento é causado por esse aprimoramento e não reflete uma degradação de desempenho. Esse aprimoramento está disponível em VDAs 1903 ou posteriores.

Passar o mouse sobre a barra de Carregamento de Perfil exibe uma dica de ferramenta mostrando os detalhes do perfil de usuário para a sessão atual.




Clique em **Detalhes** para aprofundar ainda mais em cada pasta individual na pasta raiz do perfil (por exemplo, C:/Users/username), seu tamanho e o número de arquivos (incluindo arquivos dentro de pastas aninhadas).




O detalhamento do perfil está disponível no Delivery Controller versão 7 1811 ou posterior e em VDAs 1811 ou posterior. Usando as informações de detalhamento do perfil, você pode resolver problemas que envolvem um tempo de carregamento de perfil alto. Você pode:

- Redefinir o perfil do usuário
- Otimizar o perfil removendo arquivos grandes indesejados
- Reduzir o número de arquivos para diminuir a carga da rede
- Usar streaming de perfil

Por padrão, todas as pastas na raiz do perfil são exibidas no detalhamento. Para ocultar a visibilidade da pasta, edite o seguinte valor do registro na máquina VDA:

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

1. No VDA, adicione um novo valor de registro **ProfileFoldersNameHidden** em HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Defina o valor como 1. Este valor deve ser um valor DWORD (32 bits). A visibilidade dos nomes das pastas agora está desativada.
3. Para tornar os nomes das pastas visíveis novamente, defina o valor como 0.

> **Nota:** Você pode usar comandos GPO ou PowerShell para aplicar a alteração do valor do registro em várias máquinas. Para obter mais informações sobre como usar GPO para implantar alterações de registro, consulte o blog.

Informações adicionais

- A análise detalhada do perfil não considera pastas redirecionadas.
- Os arquivos NTUser.dat na pasta raiz podem não estar visíveis para os usuários finais. No entanto, eles estão incluídos no detalhamento do perfil e exibidos na lista de arquivos em **Pasta Raiz**.
- Certos arquivos ocultos na pasta AppData não são incluídos no detalhamento do Perfil.
- O número de arquivos e os dados de tamanho do perfil podem não corresponder aos dados no painel Personalização devido a certas limitações do Windows.

### SESSÃO INTERATIVA

Sessão Interativa é o tempo necessário para "entregar" o controle do teclado e do mouse ao usuário após o carregamento do perfil do usuário. Normalmente, é a duração mais longa de todas as fases do processo de logon e é calculada como **duração da Sessão Interativa = Carimbo de Data/Hora do Evento Desktop Ready (EventId 1000 no VDA) - Carimbo de Data/Hora do Evento User Profile Loaded (EventId 2 no VDA)**. A Sessão Interativa tem três subfases: Pré-userinit, Userinit e Shell. Passe o mouse sobre Sessão Interativa para ver uma dica de ferramenta mostrando o seguinte:

- subfases
- tempo gasto para cada subfase
- atraso total cumulativo entre essas subfases

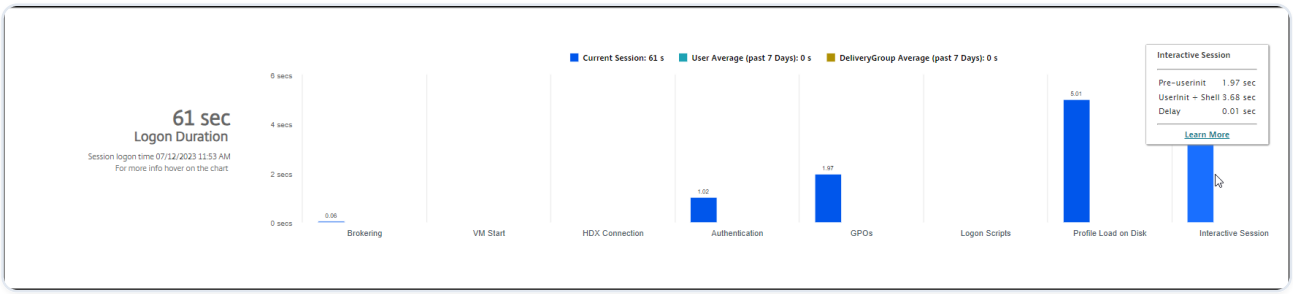
> **Nota:**
>
> Este recurso está disponível em VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores à versão 7.18 e depois atualizou para a versão 7.18 ou posterior, uma mensagem 'Detalhes indisponíveis devido a erro do servidor' é exibida. No entanto, se você iniciou sessões após a atualização, nenhuma mensagem de erro é exibida.

> Para visualizar a duração de cada subfase, habilite o rastreamento de processo de auditoria (Audit process tracking) na VM (VDA). Quando o rastreamento de processo de auditoria está desabilitado (padrão), a duração de Pre-userinit e a duração combinada de Userinit e Shell são exibidas. Você pode habilitar o rastreamento de processo de auditoria por meio de um Objeto de Política de Grupo (GPO) da seguinte forma:

1. Crie um GPO e edite-o usando o editor de GPO.

2. Vá para **Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Política de Auditoria**.
3. No painel direito, clique duas vezes em **Rastreamento de processo de auditoria**.
4. Selecione **Êxito** e clique em OK.
5. Aplique este GPO aos VDAs ou Grupo necessários.

Para obter mais informações sobre o rastreamento de processos de auditoria e como habilitá-lo ou desabilitá-lo, consulte Rastreamento de processo de auditoria na documentação da Microsoft.




Painel Duração do Logon na exibição Detalhes do Usuário.

- **Sessão Interativa – Pré-userinit:** O segmento da Sessão Interativa que se sobrepõe a Objetos de Política de Grupo e scripts. Esta subfase pode ser reduzida otimizando os GPOs e scripts.
- **Sessão Interativa – Userinit:** Quando um usuário faz logon em uma máquina Windows, o Winlogon executa userinit.exe. O Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface do usuário do Windows. Esta subfase da Sessão Interativa representa a duração entre o início do Userinit.exe e o início da interface do usuário para o desktop virtual ou aplicativo.
- **Sessão Interativa – Shell:** Na fase anterior, o Userinit inicia a inicialização da interface do usuário do Windows. A subfase Shell captura a duração entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.
- **Atraso:** Este é o atraso de tempo cumulativo entre as subfases **Pré-userinit e Userinit** e as subfases **Userinit e Shell**.

O tempo total de logon não é a soma exata dessas fases. Por exemplo, algumas fases ocorrem em paralelo e, em algumas fases, ocorre mais processamento que pode resultar em uma duração de logon mais longa do que a soma. O tempo total de logon não inclui o tempo ocioso do ICA®, que é o tempo entre o download do arquivo ICA e o lançamento do arquivo ICA para um aplicativo. Para habilitar a abertura automática do arquivo ICA após o lançamento do aplicativo, configure seu navegador para o lançamento automático do arquivo ICA após o download de um arquivo ICA. Para obter mais informações, consulte CTX804493.

> **Nota:** O gráfico Duração do Logon mostra as fases de logon em segundos. Quaisquer valores de duração abaixo de um segundo são exibidos como valores de subsegundo. Os valores acima de um segundo são arredondados para o 0,5 segundo mais próximo. O gráfico foi projetado para mostrar o valor mais alto do eixo y como 200 segundos. Qualquer valor maior que 200 segundos é mostrado com o valor real exibido acima da barra.

### Dicas de solução de problemas

Para identificar valores incomuns ou inesperados no gráfico, compare a quantidade de tempo gasto em cada fase da sessão atual com a duração média para este usuário nos últimos sete dias e a duração média para todos os usuários neste grupo de entrega nos últimos sete dias.

Escalone conforme necessário. Por exemplo, se a inicialização da VM for lenta, o problema pode estar no hipervisor, então você pode escalá-lo para o administrador do hipervisor. Ou, se o tempo de intermediação for lento, você pode escalar o problema para o administrador do site para verificar o balanceamento de carga no Delivery Controller.

Examine as diferenças incomuns, incluindo:

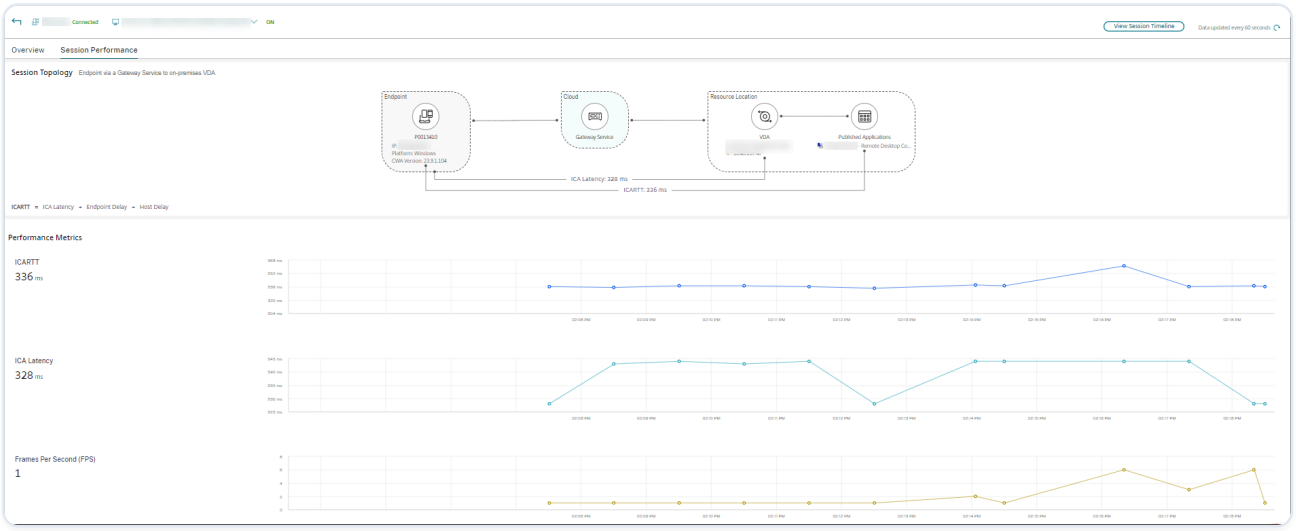
- Barras de logon (atuais) ausentes
- Grande discrepância entre a duração atual e a duração média deste usuário. As causas incluem:
  - Uma nova aplicação foi instalada.
  - Uma atualização do sistema operacional ocorreu.
  - Alterações de configuração foram feitas.
  - O tamanho do perfil do usuário é alto. Neste caso, a Carga do Perfil é alta.
- Grande discrepância entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

Se necessário, clique em **Reiniciar** para observar o processo de logon do usuário e solucionar problemas, como Inicialização da VM ou Intermediação.

## Diagnosticar problemas de desempenho da sessão

A guia **Desempenho da Sessão** na Página de Detalhes do Usuário aprimorou os fluxos de trabalho de solução de problemas para ajudar a identificar problemas nas sessões de usuário HDX™. Os painéis Topologia da Sessão e Métricas de Desempenho ajudam a correlacionar a

visualização de componentes e várias métricas de desempenho de uma sessão em uma única visualização e reduzem o tempo médio para a resolução de problemas de experiência da sessão.




### Visualização de Salto de Rede de Ponta a Ponta

A visualização de salto de rede de ponta a ponta é o próximo passo para aprimorar os fluxos de trabalho de solução de problemas. A seção **Detalhes do Usuário** > **Desempenho da Sessão** > **Topologia da Sessão** fornece uma representação visual da visualização de salto de rede de ponta a ponta para sessões HDX conectadas.

A Topologia da Sessão para uma sessão conectada mostra os componentes envolvidos no caminho da sessão com seus metadados, o link entre os componentes e os aplicativos publicados no VDA. Além disso, as seguintes métricas de desempenho da sessão são exibidas para a sessão:

- Latência ICA® - A latência é basicamente a latência da rede. Este parâmetro indica se a rede está lenta.
- ICA RTT - ICARTT é o intervalo de tempo entre a ação de um usuário e a resposta gráfica exibida em sua tela. Esta medição inclui Latência ICA, Atraso do Endpoint e Atraso do Host.

Você pode usar esta visualização para entender os componentes pelos quais os dados da sessão fluem e identificar o salto específico que pode estar causando problemas de desempenho.

As métricas de desempenho na visualização Topologia da Sessão estão disponíveis apenas para sessões HDX no estado conectado.

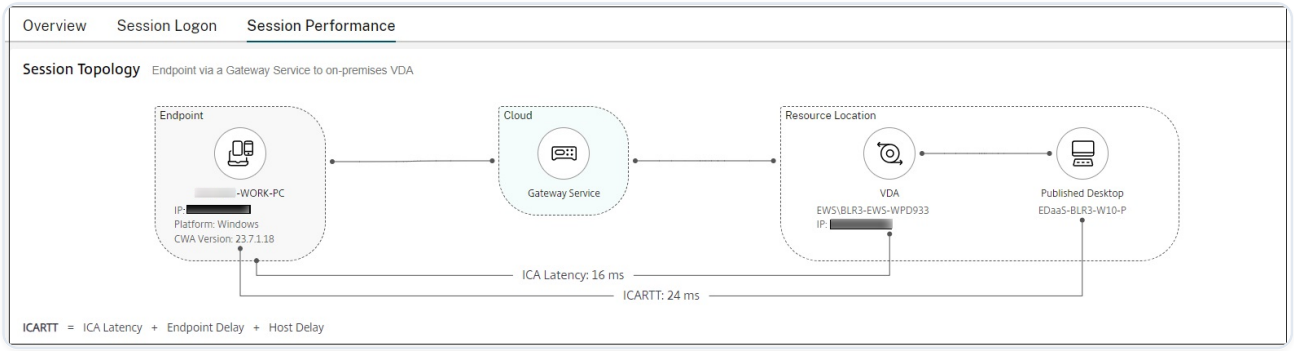
#### CENÁRIOS DE TOPOLOGIA DE SESSÃO

Dependendo do cenário de implantação do site, os componentes envolvidos em uma sessão são todos ou qualquer um dos seguintes:

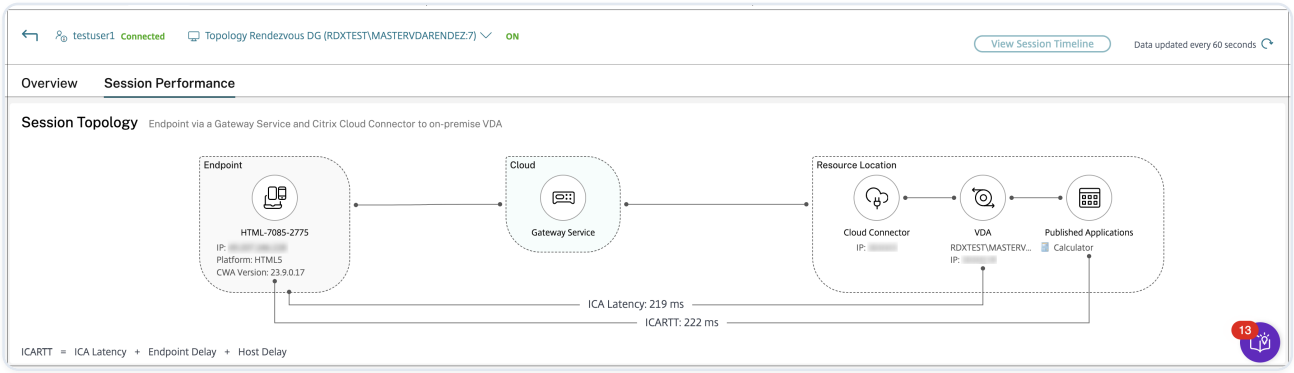
- Aplicativo Citrix Workspace™ no Ponto de Extremidade
- Serviço Gateway/Gateway local
- Cloud Connector – O Gateway está conectado ao DaaS por meio de um Cloud Connector no caso de conexões híbridas.
- VDAs

Consequentemente, as possíveis topologias de rede são as seguintes:

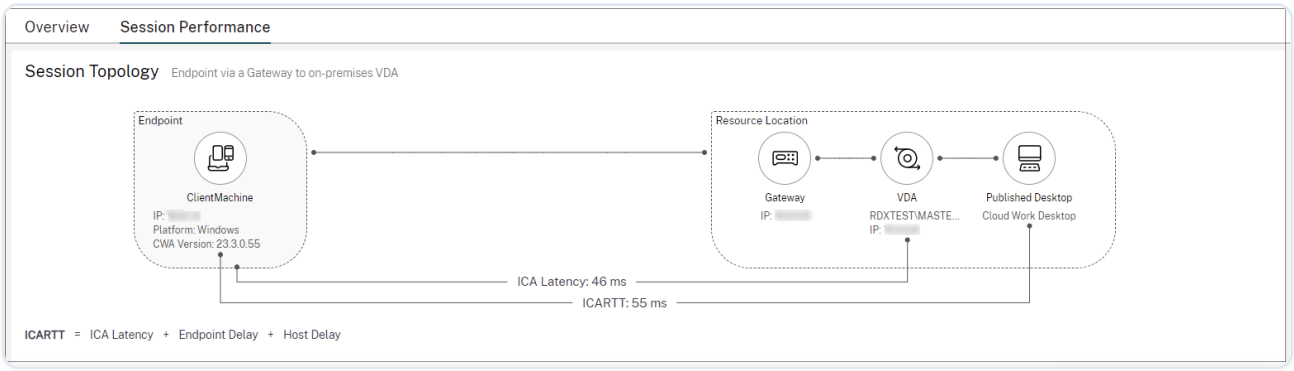
- O aplicativo Citrix Workspace no ponto de extremidade se conecta via Citrix Workspace e Gateway Service a um VDA local. Nenhum Cloud Connector é usado para se conectar ao VDA.



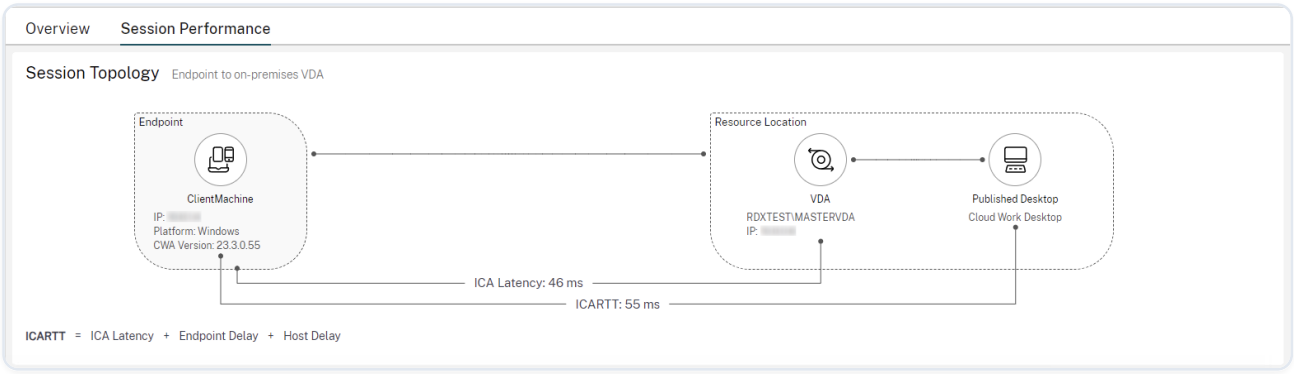

- O aplicativo Citrix Workspace no ponto de extremidade se conecta via Citrix Workspace e Gateway Service a um VDA local via Cloud Connector.




- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront™ e Gateway local a um VDA local.




- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront a um VDA local.




### Métricas de Desempenho

O painel **Métricas de Desempenho** oferece a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. As tendências para as métricas de sessão ajudam a indicar como essas métricas se comportaram ao longo do tempo. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados em tempo real, você pode visualizar os dados dos últimos 15 minutos sem esperar pelo tempo de carregamento da página. Os gráficos ajudam a correlacionar múltiplas métricas de desempenho de componentes em uma única visualização.



> **Nota:**

> Com o suporte a métricas dos últimos 15 minutos, o gráfico é plotado para a duração em que a sessão está conectada e desconectada. A métrica da sessão desconectada é exibida com o valor zero.

> Além de ICARTT e Latência ICA, as seguintes métricas estão disponíveis:

- Quadros por Segundo - Quadros por Segundo é uma métrica importante que indica a capacidade de resposta da sessão. Largura de Banda de Saída Disponível - Largura de Banda de Saída Disponível é uma medida da largura de banda total disponível para transmitir dados do VDA para o endpoint.
- Largura de Banda de Saída Consumida - Largura de Banda de Saída Consumida indica a quantidade real de dados transmitidos do VDA para o endpoint para exibir sessões aos usuários.

Analisar a Largura de Banda de Saída Disponível e a Largura de Banda de Saída Consumida ajuda a verificar se há largura de banda suficiente para atender às sessões e a detectar se uma sessão é afetada por largura de banda insuficiente.

### Usuários sombra

No Director, use o recurso de espelhamento de usuário para visualizar ou trabalhar diretamente na máquina virtual ou sessão de um usuário. Você pode espelhar VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja espelhar. Verifique isso verificando o nome da máquina listado na barra de título do usuário.

O Director inicia o espelhamento em uma nova guia, atualize as configurações do seu navegador para permitir pop-ups da URL do Director.

Acesse o recurso de espelhamento na exibição **Detalhes do Usuário**. Selecione a sessão do usuário e clique em **Espelhar** na exibição Gerenciador de Atividades ou no painel Detalhes da Sessão.

#### Espelhamento de VDAs Linux

O espelhamento está disponível para VDAs Linux Versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu Versão 16.04.

> **Observação:**

- O VDA deve estar acessível a partir da interface do usuário do Director para que o espelhamento funcione. Portanto, o espelhamento é possível apenas para VDAs Linux na mesma intranet que o cliente Director.
- O Director usa FQDN para se conectar ao VDA Linux de destino. Certifique-se de que o cliente Director possa resolver o FQDN do VDA Linux.
- O VDA deve ter os pacotes python websockify e x11vnc instalados.
- A conexão noVNC com o VDA usa o protocolo WebSocket. Por padrão, o protocolo WebSocket **ws://** é usado. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro **wss://**. Instale certificados SSL em cada cliente Director e VDA Linux.

Siga as instruções em Espelhamento de Sessão para configurar seu VDA para espelhamento.

1. Depois de clicar em **Espelhar**, a conexão de espelhamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou sessão.
3. O administrador pode apenas visualizar a sessão espelhada.

**Espelhamento de VDAs Windows**

As sessões de VDA do Windows são espelhadas usando o Assistência Remota do Windows. Habilite o recurso **Assistência Remota do Windows do Usuário** durante a instalação do VDA. Para obter mais informações, consulte Habilitar ou desabilitar recursos.

1. Depois de clicar em **Espelhar**, a conexão de espelhamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo de incidente .msrc.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ainda não estiver selecionado por padrão. Um prompt de confirmação aparece no dispositivo do usuário.
3. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou da sessão.
4. Para ter mais controle, peça ao usuário para compartilhar o controle do teclado e do mouse.

### OTIMIZAR NAVEGADORES MICROSOFT INTERNET EXPLORER PARA ESPELHAMENTO

Configure seu navegador Microsoft Internet Explorer para abrir automaticamente o arquivo Microsoft Remote Assistance (.msra) baixado com o cliente de Assistência Remota.

Para fazer isso, você deve habilitar a configuração Solicitação automática para downloads de arquivos no editor de Política de Grupo:

Configuração do Computador \> Modelos Administrativos \> Componentes do Windows \> Internet Explorer \> Painel de Controle da Internet \> Página de Segurança \> Zona da Internet \> Solicitação automática para downloads de arquivos.

Por padrão, esta opção está habilitada para sites na zona da Intranet local. Se o site do Director não estiver na zona da Intranet local, considere adicionar o site manualmente a esta zona.

### Enviar mensagens para usuários

No Director, envie uma mensagem para um usuário conectado a uma ou mais máquinas. Use este recurso para enviar avisos imediatos sobre ações administrativas, como manutenção iminente da área de trabalho, logoffs e reinícios de máquinas e redefinições de perfil.

1. Na exibição Gerenciador de Atividades, selecione o usuário e clique em Detalhes.
2. Na exibição Detalhes do Usuário, localize o painel Detalhes da Sessão e clique em Enviar Mensagem.
3. Digite as informações da sua mensagem nos campos Assunto e Mensagem e clique em Enviar.

Se a mensagem for enviada com sucesso, uma mensagem de confirmação aparecerá no Director. A mensagem aparece na máquina do usuário.

Se a mensagem não for enviada com sucesso, uma mensagem de erro aparecerá no Director. Solucione o problema de acordo com a mensagem de erro. Quando terminar, digite o assunto e o texto da mensagem novamente e clique em **Tentar** novamente.

### Resolver falhas de aplicativo

Na exibição **Activity Manager**, clique na guia Aplicativos. Você pode visualizar todos os aplicativos em todas as máquinas às quais este usuário tem acesso, incluindo aplicativos locais e hospedados para a máquina atualmente conectada, e o status de cada um.

> **Nota:**
>
> Se a guia Aplicativos estiver esmaecida, entre em contato com um administrador com permissão para habilitar a guia.

> A lista inclui apenas os aplicativos que foram iniciados dentro da sessão.

Para máquinas com SO de várias sessões e máquinas com SO de sessão única, os aplicativos são listados para cada sessão desconectada. Se o usuário não estiver conectado, nenhum aplicativo será exibido.

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| Encerrar o aplicativo que não está respondendo | Escolha o aplicativo que não está respondendo e clique em Encerrar Aplicativo. Assim que o aplicativo for encerrado, peça ao usuário para iniciá-lo novamente. |
| Encerrar processos que não estão respondendo | Se você tiver a permissão necessária, clique na guia Processos. Selecione um processo que esteja relacionado ao aplicativo ou que esteja usando uma grande quantidade de recursos de CPU ou memória e clique em Encerrar Processo. No entanto, se você não tiver a permissão necessária para encerrar o processo, a tentativa de encerrar um processo falhará. |
| Reiniciar a máquina do usuário | Apenas para máquinas com SO de sessão única, para a sessão selecionada, clique em Reiniciar. Alternativamente, na exibição Detalhes da Máquina, use os controles de energia para reiniciar ou desligar a máquina. Instrua o usuário a fazer login novamente para que você possa verificar o aplicativo novamente. Para máquinas com SO de várias sessões, a opção de reinicialização não está disponível. Em vez disso, faça logoff do usuário e permita que o usuário faça login novamente. |
| Colocar a máquina em modo de manutenção | Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina em modo de manutenção. Na exibição Detalhes da Máquina, clique em Detalhes e ative a opção |

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| | de modo de manutenção. Encaminhe para o administrador apropriado. |

### Restaurar conexões de desktop

No Director, verifique o status da conexão do usuário para a máquina atual na barra de título do usuário.

Se a conexão de desktop falhou, o erro que causou a falha é exibido e pode ajudar você a decidir como solucionar o problema.

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| Certifique-se de que a máquina não esteja em modo de manutenção | Na página Detalhes do Usuário, certifique-se de que o modo de manutenção esteja desativado. |
| Reiniciar a máquina do usuário | Selecione a máquina e clique em **Reiniciar**. Use esta opção se a máquina do usuário não estiver respondendo ou não conseguir se conectar. Por exemplo, quando a máquina está usando uma quantidade incomumente alta de recursos da CPU, o que pode tornar a CPU inutilizável. |

### Restaurar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

Na exibição Detalhes do Usuário, solucione falhas de sessão no painel **Detalhes da Sessão**. Você pode visualizar os detalhes da sessão atual, indicados pelo ID da sessão.

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| Encerrar aplicativos ou processos que não estão respondendo | Clique na guia **Aplicativos**. Selecione qualquer aplicativo que não esteja respondendo e clique em **Encerrar Aplicativo**. Da mesma forma, selecione qualquer processo correspondente que não esteja respondendo e clique em **Encerrar** |

| AÇÃO | DESCRIÇÃO |
| --- | --- |
| | **Processo**. Além disso, encerre processos que estão consumindo uma quantidade incomumente alta de memória ou recursos da CPU, o que pode tornar a CPU inutilizável. |
| Desconectar a sessão do Windows | Clique em **Controle de Sessão** e selecione **Desconectar**. Esta opção está disponível apenas para máquinas de SO de múltiplas sessões intermediadas. Para sessões não intermediadas, a opção é desabilitada. |
| Fazer logoff da sessão do usuário | Clique em **Controle de Sessão** e selecione **Logoff**. |

Para testar a sessão, o usuário pode tentar fazer logon novamente nela. Você também pode acompanhar o usuário para monitorar mais de perto esta sessão.

### Gerar relatórios do sistema de canais HDX™

Na visualização **Detalhes do Usuário**, verifique o status dos canais HDX na máquina do usuário no painel **HDX**. Este painel está disponível somente se a máquina do usuário estiver conectada usando HDX.

Se uma mensagem aparecer indicando que as informações não estão disponíveis no momento, aguarde um minuto para a página ser atualizada ou selecione o botão **Atualizar**. Os dados HDX demoram um pouco mais para serem atualizados do que outros dados.

Clique em um ícone de erro ou aviso para obter mais informações.

> Dica:
>
> Você pode visualizar informações sobre outros canais na mesma caixa de diálogo clicando nas setas esquerda e direita no canto esquerdo da barra de título.
>
> Os relatórios do sistema de canais HDX são usados principalmente pelo Suporte Citrix para solucionar problemas.

1. No painel HDX, clique em Baixar Relatório do Sistema.

2. Você pode visualizar ou salvar o arquivo de relatório .xml.
    - Para visualizar o arquivo .xml, clique em Abrir. O arquivo .xml aparece na mesma janela que o aplicativo Director.
    - Para salvar o arquivo .xml, clique em Salvar. A janela Salvar como é exibida, solicitando um local na máquina do Director para baixar o arquivo.

## Redefinir um perfil de usuário

> **CUIDADO:**

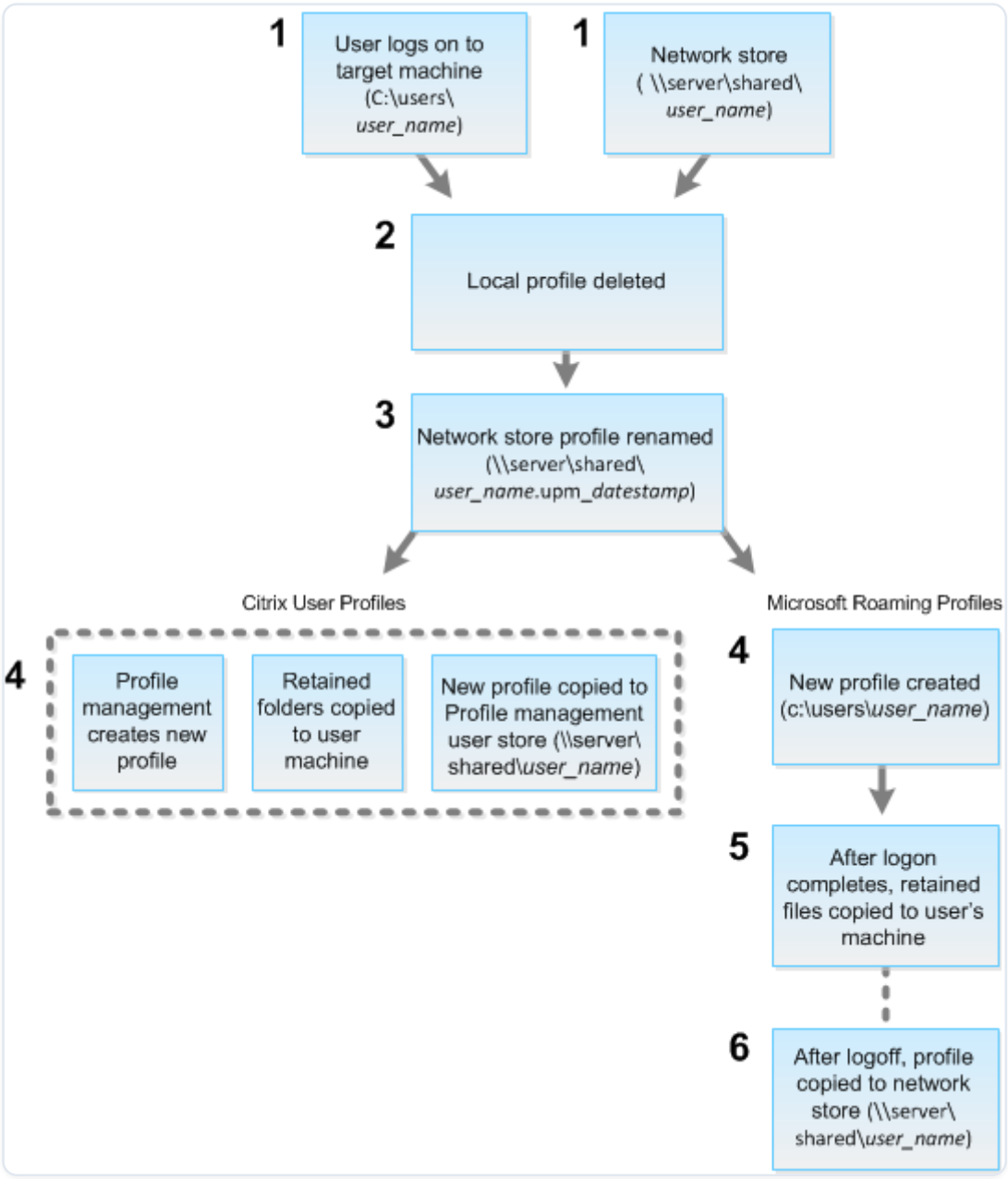
> Quando um perfil é redefinido, as pastas e arquivos do usuário são salvos e copiados para o novo perfil. No entanto, a maioria dos dados do perfil do usuário está ausente (por exemplo, o registro é redefinido e as configurações do aplicativo podem ser excluídas).

> A função de redefinição se aplica a soluções de perfil baseadas em arquivo e baseadas em contêiner.

### Como os perfis redefinidos são processados

Qualquer perfil de usuário Citrix® ou perfil móvel da Microsoft pode ser redefinido. Depois que o usuário faz logoff e você seleciona o comando de redefinição (seja no Director ou usando o SDK do PowerShell), o Director primeiro identifica o perfil de usuário em uso e emite um comando de redefinição apropriado. O Director recebe as informações por meio do Profile Management, incluindo informações sobre o tamanho do perfil, tipo e tempos de logon.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.




O comando de redefinição emitido pelo Director especifica o tipo de perfil. O serviço Profile Management então tenta redefinir um perfil desse tipo e procura o compartilhamento de rede apropriado (armazenamento de usuário). Se o usuário for processado pelo Profile Management, mas receber um comando de perfil móvel, ele será rejeitado (ou vice-versa).

1. Se um perfil local estiver presente, ele será excluído.
2. O perfil de rede é renomeado.
3. A próxima ação depende se o perfil que está sendo redefinido é um perfil de usuário Citrix ou um perfil móvel da Microsoft.

   Para perfis de usuário Citrix, o novo perfil é criado usando as regras de importação do Profile Management. As pastas são copiadas de volta para o perfil de rede, e o usuário pode fazer logon normalmente. Se um perfil móvel for usado para a redefinição, quaisquer configurações

de registro no perfil móvel serão preservadas no perfil redefinido. Você pode configurar o Profile Management para que um perfil de modelo substitua o perfil móvel, se necessário.

Para perfis móveis da Microsoft, o Windows cria um perfil e, quando o usuário faz logon, as pastas são copiadas de volta para o dispositivo do usuário. Quando o usuário faz logoff novamente, o novo perfil é copiado para o armazenamento de rede.

**Para redefinir um perfil de usuário no Director**

Se você estiver usando o Citrix Virtual Desktops™ (Desktop VDA), faça o seguinte:

1. Em **Director**, procure o usuário cujo perfil você deseja redefinir e, em seguida, selecione a sessão desse usuário.
2. Clique em **Redefinir Perfil**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente. As pastas e arquivos que foram salvos do perfil do usuário são copiados para o novo perfil.

Se você estiver usando o Citrix Virtual Desktops (Server VDA), você precisa estar logado para realizar a redefinição do perfil. O usuário então precisa fazer logoff e logon novamente para concluir a redefinição do perfil.

> **Importante:**

> Se o usuário tiver perfis em várias plataformas (como Windows 8 e Windows 7), instrua o usuário a fazer logon novamente primeiro no mesmo desktop ou aplicativo que o usuário relatou como um problema. Essa ação de logon garante que o perfil correto seja redefinido. Se o perfil for um perfil de usuário Citrix, o perfil já estará redefinido quando a área de trabalho do usuário aparecer. Se o perfil for um perfil móvel da Microsoft, a restauração da pasta ainda poderá estar em andamento por um breve período. O usuário deve permanecer logado até que a restauração seja concluída.

> Se o perfil não for redefinido com sucesso (por exemplo, o usuário não conseguir fazer logon novamente na máquina ou alguns arquivos estiverem faltando), você deve restaurar manualmente o perfil original.

Observe o seguinte:

- Se o armazenamento de usuário estiver habilitado como a solução de perfil de usuário, o novo perfil conterá as seguintes pastas pessoais do perfil de usuário original:
  - Área de Trabalho
  - Cookies
  - Favoritos
  - Documentos
  - Imagens
  - Música
  - Vídeos
- Se o contêiner de perfil do Citrix Management estiver habilitado como a solução completa de perfil de usuário, o novo perfil não conterá as pastas pessoais anteriores.
- No Windows 8 e posterior, os cookies não são copiados para o novo perfil quando os perfis são redefinidos.

**Para restaurar manualmente um perfil após uma redefinição com falha**

1. Instrua o usuário a fazer logoff de todas as sessões.
2. Exclua o perfil local, se existir.
3. Localize a pasta arquivada no compartilhamento de rede que contém a data e a hora anexadas ao nome da pasta, a pasta com uma extensão .upm_datestamp.
4. Exclua o nome do perfil atual. Ou seja, aquele sem a extensão upm_datestamp.
5. Renomeie a pasta arquivada usando o nome do perfil original. Ou seja, remova a extensão de data e hora. Você retornou o perfil ao seu estado original, antes da redefinição.

**Para redefinir um perfil usando o SDK do PowerShell**

Você pode redefinir um perfil usando o SDK do Broker PowerShell.

#### NEW-BROKERMACHINECOMMAND

Cria um comando enfileirado para entrega a um usuário, sessão ou máquina específica. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`.

#### EXEMPLOS

Consulte os exemplos a seguir para obter detalhes sobre como usar os cmdlets do PowerShell para redefinir um perfil:

Redefinir um perfil do Profile Management

- Suponha que você queira redefinir o perfil para user1. Use o comando PowerShell New-BrokerMachineCommand. Por exemplo:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **Importante:**
>
> O `CommandData $byteArray` deve estar no seguinte formato: `<SID>[,<backup path>]`. Se você não fornecer o caminho de backup, o Profile Management gerará uma pasta de backup nomeada pela data e hora atuais.

Redefinir um perfil de roaming do Windows

- Suponha que você queira redefinir o perfil de roaming para user1. Use o comando PowerShell New-BrokerMachineCommand. Por exemplo:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

# Sondagem de Aplicativos e Desktops

A sondagem de aplicativos e desktops automatiza o processo de verificação da integridade dos aplicativos e desktops publicados em um site, lançando-os serialmente usando o StoreFront. Os resultados da sondagem estão disponíveis no Director.

## Requisitos

- O Delivery Controller executa a versão 7.18 ou posterior para sondagem de aplicativos e a versão 1906 ou posterior para sondagem de desktops.
- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com o aplicativo Citrix Workspace™ para Windows versão 1808 ou posterior para sondagem de aplicativos e versão 1906 ou posterior para sondagem de desktops. O aplicativo Workspace para Unified Windows Platform (UWP) não é compatível.

- O Citrix Probe Agent oferece suporte à autenticação via StoreFront e Citrix Workspace usando credenciais do Active Directory. Nos casos em que o dispositivo de endpoint está conectado ao StoreFront/Workspace via Citrix Gateway, você pode autenticar usando as credenciais de domínio do Citrix Gateway ou autenticação multifator (MFA). O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como Single Sign-On (SSO).
- Certifique-se de que o Microsoft .NET Framework versão 4.7.2 ou posterior esteja instalado na máquina de endpoint onde você deseja instalar o Probe Agent.

Contas de usuário/permissões necessárias para executar a Sondagem:

- Um usuário StoreFront exclusivo para sondar em cada máquina endpoint. O usuário StoreFront não precisa ser um administrador; as sondagens podem ser executadas em um contexto de não administrador.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint.
- O usuário deve ser membro do mesmo domínio que os VDAs usados para o lançamento de aplicativos ou desktops. O Probe Agent atualmente não oferece suporte a vários domínios.
- Reutilizar contas de usuário existentes para sondagem pode desconectar os usuários de suas sessões ativas. Uma conta de usuário administrador completa ou uma função personalizada com as seguintes permissões:
    - Permissões de grupo de entrega:
        - Somente leitura
    - Permissões do Director:
        - Criar\\Editar\\Remover Configuração do Servidor de E-mail de Alerta - se o servidor de e-mail ainda não estiver configurado
        - Criar\\Editar\\Remover Configurações de Sondagem
        - Visualizar página de Configurações
        - Visualizar página de Tendências

## Configuração

Você pode agendar suas sondagens para serem executadas durante horários de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar

problemas relacionados aos aplicativos, máquina de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 e posterior oferece suporte à agregação de sites. Ao configurar o Citrix Probe Agent, selecione a opção Workspace (StoreFront) Site Aggregation Enabled para habilitar a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

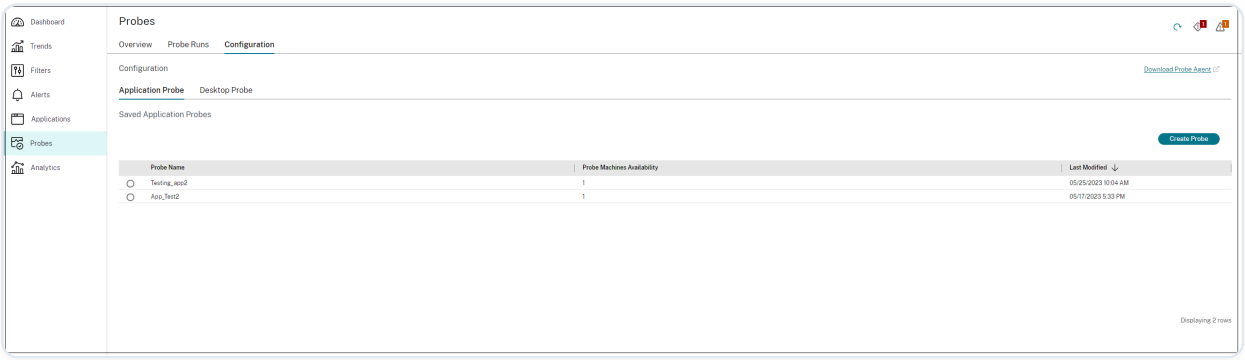
- Vários sites locais com uma URL do StoreFront.
- Sites locais e na nuvem com uma URL do StoreFront ou Workspace.
- Vários sites na nuvem com uma URL do Workspace.
- Sites locais conectados ao StoreFront ou Workspace via Citrix Gateway.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar sondas que tenham acesso a apenas um site.

### Etapa 1: Instalar e configurar o Citrix Probe Agent

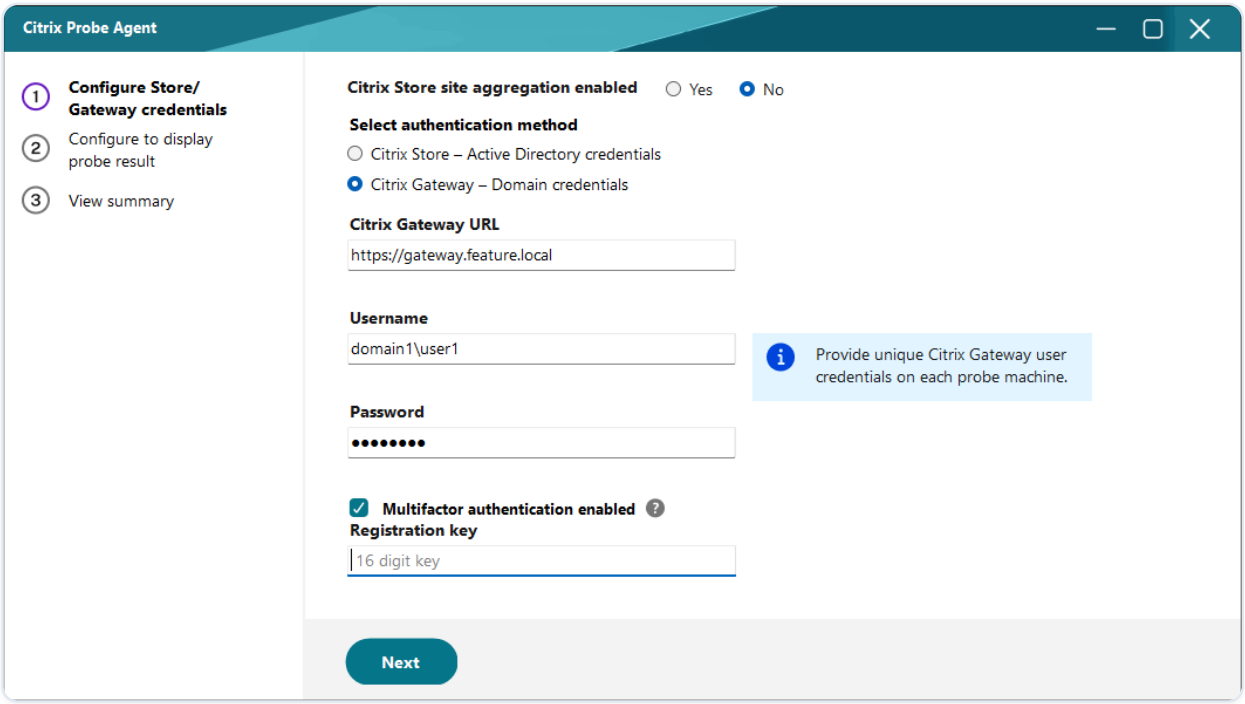
O Citrix Probe Agent é um executável do Windows que simula o lançamento real de um aplicativo ou desktop pelo usuário através do StoreFront. Ele testa os lançamentos conforme configurado no Director e reporta os resultados de volta ao Director.

1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`. O link para download também está disponível na guia **Probes** no Director.

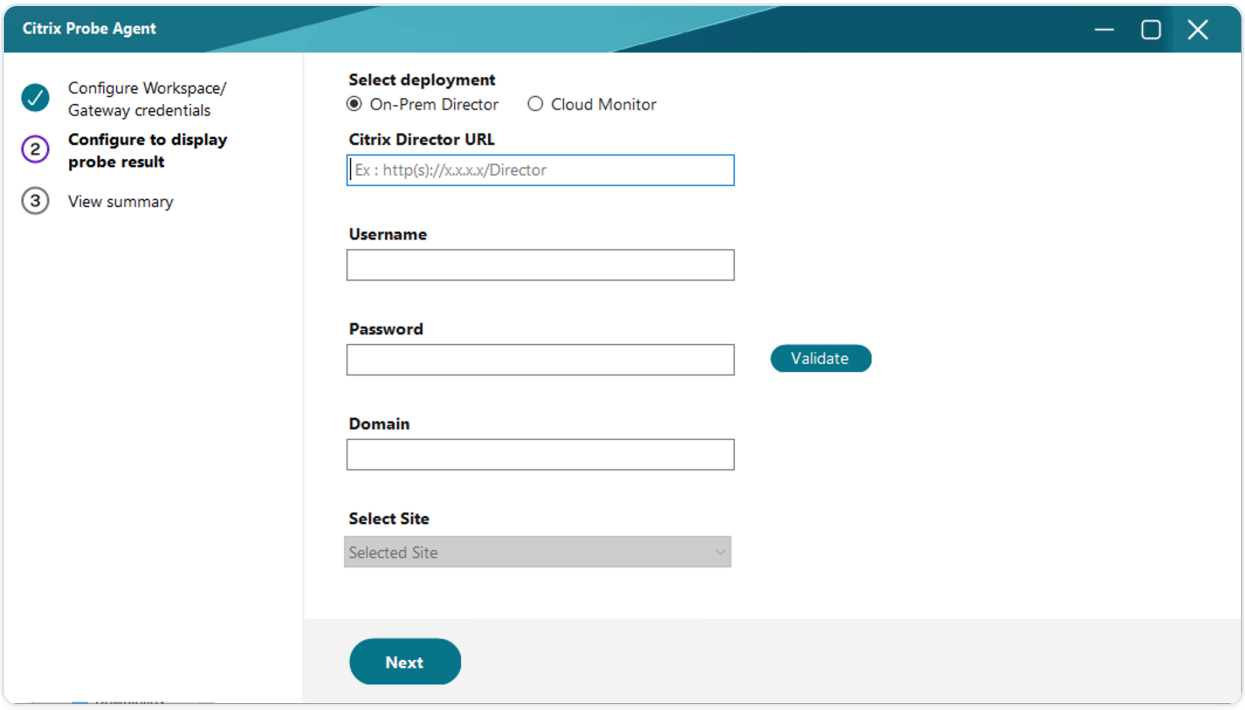



.

3. Se você tiver sites agregados, selecione a opção Workspace (StoreFront) Site Aggregation Enabled para habilitar a enumeração de aplicativos e desktops de sites agregados.
4. Selecione um método de autenticação e insira as credenciais relevantes. As credenciais são criptografadas e armazenadas com segurança.
5. Configure com suas credenciais do StoreFront Active Directory. Configure um usuário Workspace (StoreFront) exclusivo em cada máquina endpoint.
6. Escolha a opção Citrix Gateway se seu endpoint estiver conectado ao StoreFront via Citrix Gateway e configure com suas credenciais de Domínio do Citrix Gateway.




7. Escolha a opção de Autenticação Multifator se o seu Gateway a suportar e insira a chave de autenticação de 16 dígitos. Isso está disponível apenas para o Citrix Gateway configurado com LDAP e OTP Nativo usando o Esquema de Login Único.
8. Na guia **Configure To Display Probe Result**, insira suas credenciais do Director e clique em **Validate**.




9. Selecione seu site e clique em **Avançar**.
10. Na guia **Visualizar Resumo**, certifique-se de que os detalhes configurados estejam precisos. Se precisar fazer alterações, vá para a guia respectiva e faça as atualizações.

> **Observação:**

Você pode usar o script PowerShell contido em Automating Citrix Probe Agent Installation and Configuration para automatizar a instalação e configuração do Citrix Probe Agent.

### Etapa 2: Configurar Sondagem no Director

> **Limitação:**

A sondagem falha se aplicativos ou desktops forem iniciados para teste a partir de VDAs Windows que têm o banner de mensagem de logon interativo ativado. Isso ocorre porque um tempo limite é atingido devido à espera para aceitar a mensagem de logon interativo. Para desativar a mensagem de logon em um VDA de Servidor. Vá para Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança.

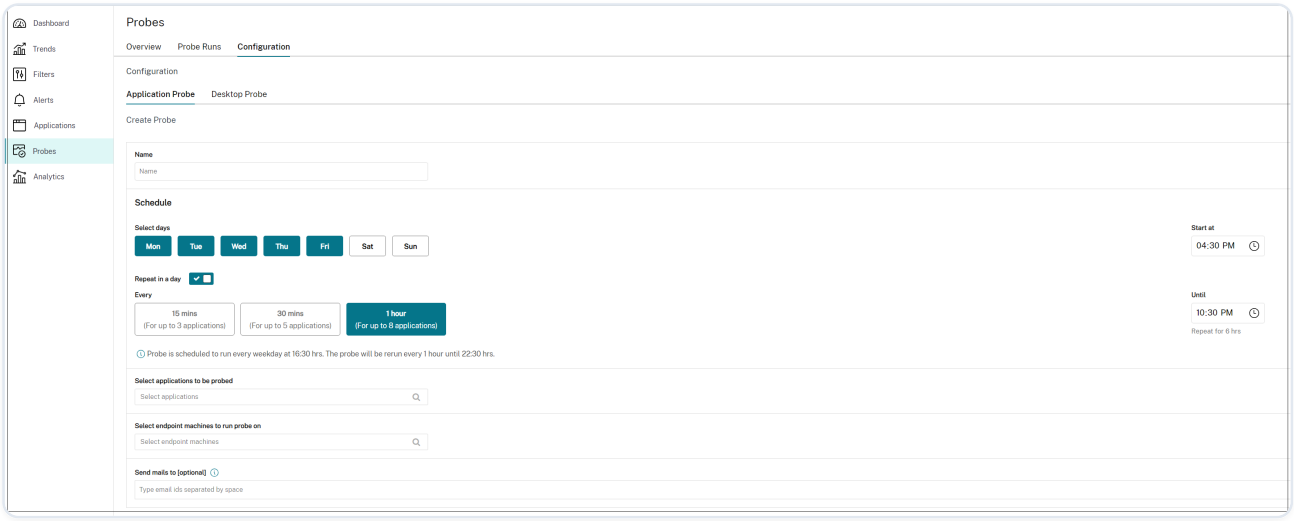
Remova o texto nos seguintes campos e atualize a política da Microsoft.

- Logon Interativo: Texto da Mensagem para usuários tentando fazer logon
- Logon Interativo: Título da Mensagem para usuários tentando fazer logon

Atribua o usuário da sonda a este VDA de Servidor específico com o banner de mensagem de logon interativo desabilitado para garantir que a sonda possa passar do estado de Inicialização de Aplicativo ou Área de Trabalho.

Para obter mais informações, consulte `<https://learn.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`.

1. Vá para **Sondas** \> **Sonda de Aplicativo** ou **Sonda de Área de Trabalho** e clique em **Criar Sonda**.
2. Na página **Criar Sondagem**, insira o nome da sondagem.
3. Selecione o agendamento:
    a. Escolha os dias da semana em que você deseja que a sondagem seja executada.
    b. Insira a hora de início em que você deseja que a sondagem seja executada.
    c. Além disso, você pode escolher a opção **Repetir em um dia**. Insira a hora de término e o intervalo em que você deseja que a sondagem se repita dentro de um dia. Por exemplo, a configuração abaixo ajuda a executar sondagens de aplicativos das 12:08 horas até as 16:34 horas, repetindo a cada 30 minutos todas as segundas, quartas, quintas e domingos.
4. Selecione o número recomendado de aplicativos ou desktops a serem sondados, dependendo do intervalo.
5. Selecione as máquinas de endpoint nas quais a sondagem deve ser executada.
6. Insira os endereços de e-mail dos administradores para enviar os resultados das sondagens com falha. Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.




Nesta configuração, as sessões do aplicativo são iniciadas às 12:08, 12:38, 13:08 e assim por diante até as 16:08, todas as segundas, quartas, quintas e domingos.

**Observação:**

- Após a configuração, o agente executa as sondagens configuradas a partir da próxima hora.
- As sondagens que foram configuradas antes da introdução da opção **Repetir em um dia** continuam a ser executadas no horário agendado. Elas têm a opção **Repetir em um dia** desativada por padrão.
- Recomenda-se que você configure as sondagens de forma que cada execução tenha um período de 5 minutos para evitar sobreposições.

### Etapa 3: Execução da sonda

O agente executa a sondagem de acordo com a configuração da sonda que ele busca periodicamente do Director.

Ele inicia os aplicativos selecionados serialmente usando o StoreFront. O agente reporta os resultados de volta ao Director via banco de dados do Monitor. As falhas são relatadas em cinco estágios específicos:

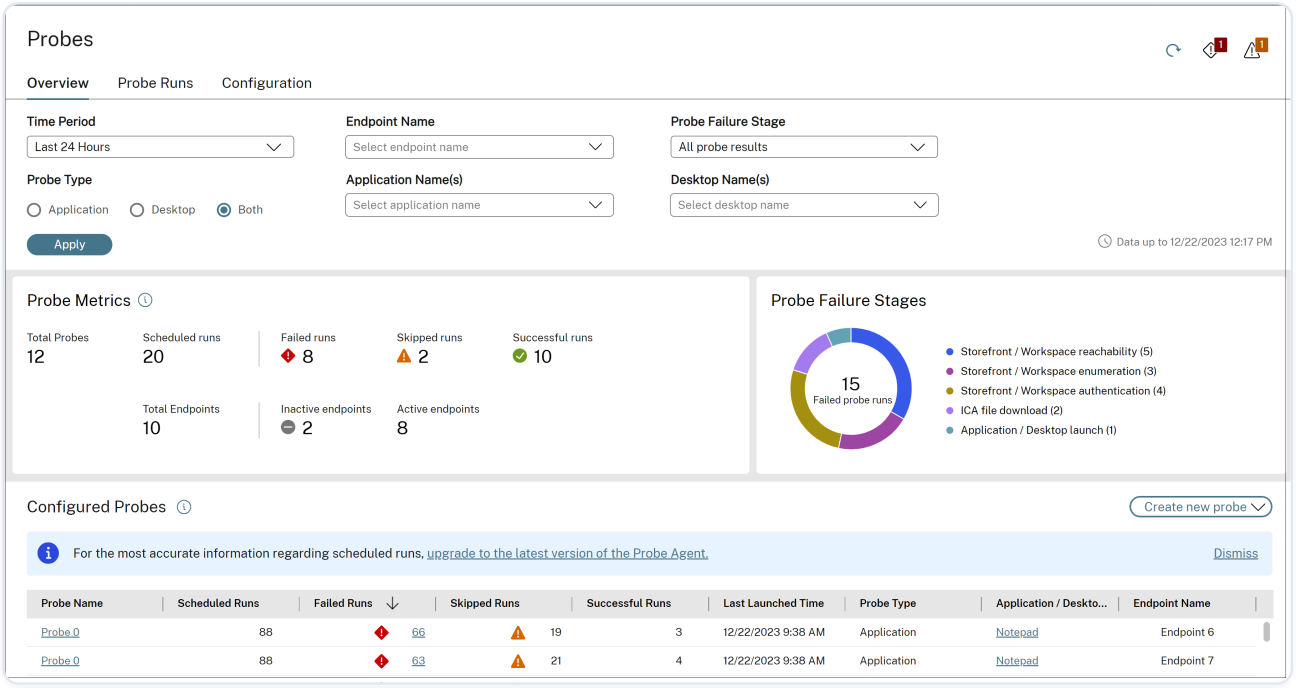
- **Acessibilidade do StoreFront** - a URL do StoreFront configurada não está acessível.
- **Autenticação do StoreFront** - as credenciais do StoreFront configuradas são inválidas.
- **Enumeração do StoreFront** - a lista de aplicativos de Enumeração do StoreFront não contém o aplicativo ou área de trabalho a ser sondado.

- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização de Aplicativo / Desktop** – o aplicativo ou desktop não pôde ser iniciado.

### Etapa 4: Visualizar resultados da sonda

Você pode ver os resultados da sonda em **Sondas**. A visualização Sondas oferece uma visão abrangente dos resultados da sonda. Esses resultados ajudam a analisar e solucionar problemas proativamente, permitindo uma experiência de inicialização de sessão mais suave para os usuários.

A guia **Visão Geral** fornece um resumo de todas as sondas configuradas em uma única visualização.




Você pode filtrar sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Tipo de Resultado da Sonda. As sondas que correspondem aos critérios de filtro são mostradas com os seguintes detalhes por sonda, aplicativo/desktop e endpoint.

**Métricas da Sonda** mostra a contagem de execuções Agendadas, Planejadas, Ignoradas, Bem-sucedidas e Falhas.

- Execuções Concluídas – o número de execuções da sonda que foram concluídas.
- Execuções com Falha – o número de execuções da sonda que falharam.
- Execuções Ignoradas – o número de execuções que não foram concluídas devido ao endpoint estar inativo ou aos serviços estarem indisponíveis.

- Execuções Bem-sucedidas – o número de sondas que foram concluídas com sucesso, sem falhas em nenhuma etapa durante o lançamento do aplicativo/desktop.

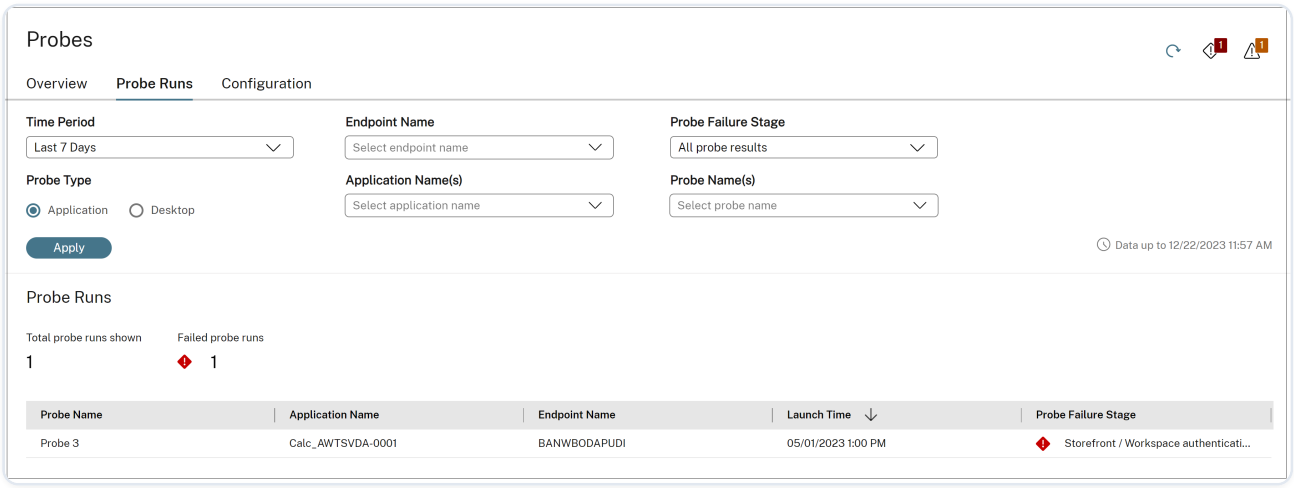
O número total de máquinas de ponto de extremidade também é exibido, com a contagem de máquinas ativas e inativas.

**Estágios de Falha da Sonda** apresenta uma análise visual da distribuição de falhas para cada grupo de falhas. Ao analisar os estágios em que a maioria das falhas ocorreu, torna-se mais fácil interpretar os resultados da sonda e solucionar problemas. A representação gráfica mostra o número de execuções de sonda com falha para o lançamento de aplicativo/desktop, downloads de arquivos ICA, enumeração do Storefront/Workspace, acessibilidade do Storefront/Workspace e autenticação do Storefront/Workspace.

Ajuda a analisar os estágios em que a maioria das falhas ocorreu. Essas informações ajudam a entender rapidamente os resultados da sonda e a solucionar problemas.

Algumas execuções de sonda podem não ser concluídas devido ao endpoint estar inativo ou aos serviços estarem indisponíveis.

A guia **Execuções de Sonda** fornece os resultados das execuções de sonda concluídas em detalhes. Você pode detalhar para ver os detalhes de cada execução individual de uma sonda selecionada. Você pode filtrar e analisar ainda mais com base em pontos de pivô importantes.




Você pode filtrar as execuções de sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Estágio de Falha da Sonda. O Estágio de Falha da Sonda exibe o estágio em que a sonda falhou. Clicar nos links Nome da Sonda, Execuções Agendadas, Execuções com Falha, Nome do Aplicativo/Desktop também o leva à página Execuções de Sonda com a lista de execuções de sonda que correspondem aos critérios de filtro.

# Matriz de compatibilidade de recursos

O Citrix Director 7 2402 é compatível com:

- Citrix Virtual Apps and Desktops™ 7 2112 e posterior
- Citrix Aplicativos Virtuais e Desktops 7 1912 LTSR

Em cada site, embora você possa usar o Director com versões anteriores do Delivery Controller™, todos os recursos da versão mais recente do Director podem não estar disponíveis. A Citrix recomenda que o Director, o Delivery Controller e os VDAs estejam na mesma versão.

> **Observação:**
>
> Depois de atualizar um Delivery Controller, você será solicitado a atualizar o site ao abrir o Studio. Para obter mais informações, consulte a seção **Sequência de atualização** em Atualizar uma implantação.

> Na primeira vez que você fizer login após uma atualização do Director, uma verificação de versão é realizada nos sites configurados. Se algum site estiver executando uma versão do Controller anterior à do Director, uma mensagem aparece no console do Director, recomendando uma atualização do site. Além disso, enquanto a versão do site for mais antiga que a do Director, uma nota permanece exibida no Painel do Director indicando essa incompatibilidade.

> **Observação:**
>
> Versões anteriores do Citrix Director não exibem políticas aplicadas a sessões de usuário executadas em versões recentes do VDA. O Citrix Director 1912 e versões anteriores não exibem políticas aplicadas a sessões de usuário executadas em versões do VDA 2003 e posteriores. Use as versões 2003 e posteriores do Citrix Director para visualizar essas políticas.

> Recursos específicos do Director com a versão mínima do Delivery Controller (DC), VDA e outros componentes dependentes necessários, juntamente com a Edição da Licença, estão listados na tabela a seguir:

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| 2311 | Reproduzir sessões ao vivo e gravadas | VDA 2308 e DDC 2311 | Todas |
| 2311 | Topologia da Sessão | Nenhum | Todos |
| 2311 | Resolução de tela ideal | Nenhum | Todos |
| 2311 | Otimização do MS Teams | VDA 2311 e DDC mais recente | Todos |
| 2311 | Aprimoramentos da Visão Geral de Probes | Nenhum | Todos |
| 2311 | Visualização de Duração de Logon de Sessão reformulada | Nenhum | Todos |
| 2308 | Resumo e detalhamento de sondas | Nenhum | Todos |
| 2308 | Suporte do Citrix Probe Agent para autenticação multifator do Citrix Gateway | Citrix Gateway | Todos |
| 2308 | Desabilitar Alertas de Hypervisor | Nenhum | Todos |
| 2308 | Tendências para métricas de experiência da sessão | Nenhum | Todos |

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| 2305 | Suporte à autenticação via Citrix Gateway | Nenhum | Todos |
| 2305 | Gerenciamento de Autoscale no Director | Nenhum | Todos |
| 2303 | Alerta de Máquinas com Falha(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/director/site-analytics/alerts-notifications.html#failed-machines-in-) | DC 7 2303 | Premium |
| 2203 | Suporte a TLS 1.3 | - | Todos |
| 2212 | Utilização de GPU em tempo real disponível para GPUs AMD | DC 7.14 e VDA 7.14 executando Windows de 64 bits e HDX 3D Pro ativado | Todos |
| 2212 | Agendamento Avançado de Sondas(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/director/probes.html) | DC 7 1906 e Citrix Probe Agent 2209 | Premium |
| 1909 | Configurar sites locais com o Citrix Analytics for Performance(/pt-br/citrix-virtual-apps-desktops/2402-ltsr/director/install-and- | DC 7 1906 e VDA 1906 | Todos |

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| | configure/ onboarding.html) | | |
| 1906 | Reconexão Automática de Sessão | DC 7 1906 e VDA 1906 | Todos |
| 1906 | Duração da inicialização da sessão | DC 7 1906 e VDA 1903 | Todos |
| 1906 | Sondagem de desktop | DC 7 1906 e Citrix Probe Agent 1903 | Premium |
| 7.9 e posterior | Duração do Citrix Profile Management no Carregamento de Perfil | VDA 1903 | Todos |
| 1811 | Detalhamento de Perfil | DC 7 1811 e VDA 1811 | Todos |
| 1811 | Monitoramento de Alertas do Hypervisor | DC 7 1811 | Premium |
| 1811 | Sondagem de aplicativos | DC 7 1811 e Citrix Application Probe Agent 1811 | Premium |
| 1811 | Integridade da licença RDS da Microsoft | DC 7 1811 e VDA 7.16 | Todos |
| 1811 | Exibição de dados RTOP principais | DC 7 1811 e VDA 1808 | Premium |
| 1808 | Exportação de dados de filtros | DC 7 1808 | Todos |

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| 1808 | Detalhes da sessão interativa | DC 7 1808 e VDA 1808 | Todos |
| 1808 | Detalhes da GPO | DC 7 1808 e VDA 1808 | Todos |
| 1808 | Dados históricos da máquina disponíveis usando a API OData | DC 7 1808 | Todos |
| 7.18 | Sondagem de aplicativos | DC 7.18 | Premium (anteriormente Platinum) |
| 7.18 | Políticas de alerta inteligente | DC 7.18 | Premium (anteriormente Platinum) |
| 7.18 | Link do Assistente de Saúde | Nenhum | Todos |
| 7.18 | Detalhamento da Sessão Interativa | Nenhum | Todos |
| 7.17 | Autenticação de cartão inteligente PIV | Nenhum | Todos |
| 7.16 | Análise de Aplicativos | DC 7.16 e VDA 7.15 | Todos |
| 7.16 | API OData V.4 | DC 7.16 | Todos |
| 7.16 | Usuários do VDA Linux Shadow | VDA 7.16 | Todos |
| 7.16 | Suporte a grupos locais de domínio | Nenhum | Todos |

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| 7.16 | Acesso ao console da máquina | DC 7.16 | Todos |
| 7.15 | Monitoramento de falhas de aplicativos | DC 7.15 e VDA 7.15 | Todos |
| 7.14 | Solução de problemas centrada em aplicativos | DC 7.13 e VDA 7.13 | Todos |
| 7.14 | Monitoramento de Disco | DC 7.14 e VDA 7.14 | Todos |
| 7.14 | Monitoramento de GPU | DC 7.14 e VDA 7.14 | Todos |
| 7.13 | Protocolo de transporte no painel Detalhes da Sessão | DC 7.x e VDA 7.13 | Todos |
| 7.12 | Descrições amigáveis de falhas de conexão e máquina | DC 7.12 e VDA 7.x | Todos |
| 7.12 | Disponibilidade aprimorada 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 | Relatório de utilização de recursos | DC 7.11 e VDA 7.11 | Todos |

| VERSÃO DO DIRECTOR | RECURSO | DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA | EDIÇÃO |
|---|---|---|---|
| 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 no relatório de exportação | DC 7.11 e VDA 7.x | Todos |
| 7.11 | Integração com Citrix ADM | DC 7.11, VDA 7.x e MAS versão 11.1 Build 49.16 | Premium (anteriormente Platinum) |
| 7.9 | Detalhes 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) |
| 7.7 | Integração de Autenticação do Windows | DC 7.x e VDA 7.x | Todos |
| 7.7 | Uso de SO de Sessão Única e Múltiplas Sessões | DC 7.7 e VDA 7.x | Premium (anteriormente Platinum) |
| 7.6.300 | Suporte para canal virtual Framehawk | DC 7.6 e VDA 7.6 | Todos |
| 7.6.200 | Integração de gravação de sessão | DC 7.6 e VDA 7.x | Premium (anteriormente Platinum) |
| 7 | Integração HDX Insight | DC 7.6, VDA 7.x e Citrix ADM | Premium (anteriormente Platinum) |

# Granularidade e retenção de dados

## Agregação de valores de dados

O Serviço de Monitoramento coleta vários dados, incluindo uso de sessão do usuário, detalhes de desempenho de logon do usuário, detalhes de balanceamento de carga da sessão e informações de falha de conexão e máquina. Os dados são agregados de forma diferente dependendo de sua categoria. Compreender a agregação de valores de dados apresentados usando as APIs do Método OData é fundamental para interpretar os dados. Por exemplo:

- Sessões Conectadas e Falhas de Máquina ocorrem durante um período. Portanto, são expostas como máximos durante um período de tempo.
- A Duração do Logon é uma medida da duração do tempo, portanto, é exposta como uma média durante um período de tempo.
- A Contagem de Logons e as Falhas de Conexão são contagens de ocorrências durante um período, portanto, são expostas como somas durante um período de tempo.

## Avaliação de dados concorrentes

As sessões devem ser sobrepostas para serem consideradas concorrentes. No entanto, quando o intervalo de tempo é de 1 minuto, todas as sessões nesse minuto (independentemente de se sobreporem) são consideradas concorrentes. O tamanho do intervalo é tão pequeno que a sobrecarga de desempenho envolvida no cálculo da precisão não compensa o valor adicionado. Se as sessões ocorrerem na mesma hora, mas não no mesmo minuto, elas não são consideradas sobrepostas.

## Correlação de tabelas de resumo com dados brutos

O modelo de dados representa métricas de duas maneiras diferentes:

- As tabelas de resumo representam visualizações agregadas das métricas em granularidades de tempo por minuto, hora e dia.
- Os dados brutos representam eventos individuais ou o estado atual rastreado na sessão, conexão, aplicativo e outros objetos.

Ao tentar correlacionar dados entre chamadas de API ou dentro do próprio modelo de dados, é importante entender os seguintes conceitos e limitações:

- **Nenhum dado de resumo para intervalos parciais.** Os resumos de métricas são projetados para atender às necessidades de tendências históricas ao longo de longos períodos de tempo.

Essas métricas são agregadas na tabela de resumo para intervalos completos. Não há dados de resumo para um intervalo parcial no início (dados mais antigos disponíveis) da coleta de dados nem no final. Ao visualizar agregações de um dia (Intervalo=1440), isso significa que os primeiros e os mais recentes dias incompletos não possuem dados. Embora dados brutos possam existir para esses intervalos parciais, eles nunca são resumidos. Você pode determinar o intervalo agregado mais antigo e mais recente para uma granularidade de dados específica puxando o min e o max SummaryDate de uma tabela de resumo específica. A coluna SummaryDate representa o início do intervalo. A coluna Granularity representa a duração do intervalo para os dados agregados.

- **Correlação por tempo.** As métricas são agregadas na tabela de resumo para intervalos completos, conforme descrito na seção anterior. Elas podem ser usadas para tendências históricas, mas os eventos brutos podem estar mais atualizados no estado do que o que foi resumido para análise de tendências. Qualquer comparação baseada em tempo de dados de resumo com dados brutos deve considerar que não há dados de resumo para intervalos parciais que possam ocorrer ou para o início e fim do período de tempo.
- **Eventos perdidos e latentes.** As métricas que são agregadas na tabela de resumo podem ser ligeiramente imprecisas se os eventos forem perdidos ou latentes para o período de agregação. Embora o Serviço de Monitoramento tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo para eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a alta disponibilidade de conexão, haverá lacunas nas contagens de dados de resumo das conexões atuais, mas as instâncias de sessão ainda estarão em execução nos dados brutos.
- **Períodos de retenção de dados.** Os dados nas tabelas de resumo são retidos em um cronograma de limpeza diferente do cronograma para dados de eventos brutos. Os dados podem estar ausentes porque foram removidos das tabelas de resumo ou brutas. Os períodos de retenção também podem diferir para diferentes granularidades de dados de resumo. Dados de granularidade mais baixa (minutos) são limpos mais rapidamente do que dados de granularidade mais alta (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles poderão ser encontrados em uma granularidade mais alta. Como as chamadas de API retornam apenas a granularidade específica solicitada, não receber dados para uma granularidade não significa que os dados não existam para uma granularidade mais alta para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de data/hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não se

enquadram nos limites por hora, pode haver alguma discrepância quanto ao local onde os dados são agregados.

## Granularidade e retenção

A granularidade dos dados agregados recuperados pelo Director é uma função do período de tempo (T) solicitado. As regras são as seguintes:

- 0 \< T \<= 1 hora - usa granularidade por minuto
- 0 \< T \<= 30 dias - usa granularidade por hora
- T \> 31 dias - usa granularidade por dia

Os dados solicitados que não vêm de dados agregados vêm das informações brutas de Sessão e Conexão. Esses dados tendem a crescer rapidamente e, portanto, têm sua própria configuração de limpeza. A limpeza garante que apenas dados relevantes sejam mantidos a longo prazo. A limpeza garante melhor desempenho, mantendo a granularidade necessária para relatórios. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção, caso contrário, o padrão é usado. Caso haja perda de conectividade com o banco de dados do Site, o Serviço de Monitoramento usará os dias de retenção padrão para o direito Premium, conforme especificado na tabela abaixo.

Para acessar as configurações, execute os seguintes comandos PowerShell no Delivery Controller™:

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Tabelas MonitorData.Session e | Essa configuração afeta os | 90 | 31 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | | Monitordata.Connection | detalhes da sessão, Duração do Logon por Sessão do Usuário, tabelas de Uso Baseado em Aplicativo na página Tendências. | | |
| 2 | GroomFailuresRetentionDays | MonitorData.MachineFailureLog e MonitorData.ConnectionFailureLog | Página Tendências: Essa configuração afeta gráficos e tabelas na guia de falhas. | 90 | 31 |
| 3 | GroomLoadIndexesRetentionDays | MonitorData.LoadIndex | Essa configuração afeta os dados exibidos na guia "Índice do Avaliador de Carga" na página Tendências. | 3 | 3 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| 4 | GroomDeletedRetentionDays | Entidades MonitorData.Machine, MonitorData.Catalog, MonitorData.DesktopGroup e MonitorData.Hypervisor que têm um LifecycleState de 'Deleted'. Essa configuração também exclui quaisquer registros relacionados de Session, SessionDetail, Summary, Failure ou LoadIndex. | Entidades de Máquina, Catálogo, Grupo de Área de Trabalho e Hypervisor que têm um LifecycleState de ‘Excluído’. Essa configuração também exclui quaisquer registros relacionados de Sessão, Detalhe da Sessão, Resumo, Falha ou Índice de Carga. | 90 | 31 |
| 5 | GroomSummariesRetentionDays | MonitorData.DesktopGroupSummary, MonitorData.FailureLogSummary, e | Essa configuração afeta todos os dados do gráfico na | 365 | 31 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | | MonitorData.LoadIndexSummary | página Tendências. | | |
| 6 | GroomMachineHotfixLogRetentionDays | MonitorData.Hotfix | Essa configuração afeta os dados de hotfix do VDA mostrados na página Detalhes da Máquina. | 90 | 31 |
| 7 | GroomMinuteRetentionDays | Todas as tabelas de resumo | Essa configuração afeta os gráficos para o Período de Tempo "Últimas 2 Horas" exibido na página Tendências. | 3 | 3 |
| 8 | GroomHourlyRetentionDays | todas as tabelas de resumo | Isso afeta os gráficos semanais exibidos na página Tendências. | 32 | 31 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| 9 | GroomApplicationInstanceRetentionDays | MonitorData.ApplicationInstance | Essa configuração afeta o gráfico e as tabelas na guia Gerenciamento de capacidade e as tabelas de uso de aplicativos na página Tendências. | 90 | Não aplicável |
| 10 | GroomNotificationLogRetentionDays | MonitorData.NotificationLog | Essa configuração afeta os Alertas mostrados no Monitor. | 90 | Não aplicável |
| 11 | GroomResourceUsageRawDataRetentionDays | MonitorData.Resourceutilization | Essa configuração afeta os gráficos de CPU e Memória vistos na página Detalhes da Máquina de "Utilização Histórica da Máquina". | 3 | 3 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| 12 | GroomResourceUsageMinuteDataRetentionDays | MonitorData.ResourceUtilizationSummary | Essa configuração afeta os gráficos de CPU e Memória para o Período de Tempo de "Últimas 2 Horas" vistos na página Detalhes da Máquina de “Utilização Histórica da Máquina”. | 7 | 7 |
| 13 | GroomResourceUsageHourDataRetentionDays | MonitorData.Resourceutilizationsummary | Esta configuração afeta os gráficos de CPU e Memória vistos na página de Detalhes da Máquina de "Utilização Histórica da Máquina". | 30 | 30 |
| 14 | GroomResourceUsageD | MonitorData.Resourceuti | Esta configuraçã | 365 | 31 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | ayDataRetentionDays | lizationsummary | o afeta o gráfico de CPU e Memória visto em "Utilização de recursos" da Máquina na página Tendências e na página "Utilização da máquina" para uma máquina específica. | | |
| 15 | GroomProcessUsageRawDataRetentionDays | MonitorData.ProcessUtilization | Esta configuração afeta as informações de tendência de recursos por processo exibidas na página de uso histórico da máquina. | 1 | 1 |
| 16 | GroomProcessUsageMinuteDataRetentionDays | MonitorData.ProcessUtilizationMinuteSummary | Essa configuração afeta os gráficos de uso de CPU | 3 | 3 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | | | e Memória por processo para as "Últimas 2 Horas" mostrados na página Utilização Histórica da Máquina. | | |
| 17 | GroomProcessUsageHourDataRetentionDays | MonitorData.ProcessUtilizationHourSummary | Essa configuração afeta a tendência de uso de CPU e Memória por processo mostrada na página de uso histórico da máquina. | 7 | 7 |
| 18 | GroomProcessUsageDayDataRetentionDays | MonitorData.ProcessUtilizationDaySummary | Essa configuração afeta a tendência de uso de CPU e Memória por processo mostrada na página de | 30 | 30 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | | | uso histórico da máquina. | | |
| 19 | GroomSessionMetricsDataRetentionDays | MonitorData.Sessionmetrics | Essa configuração afeta todos os gráficos vistos na guia "Desempenho da Sessão" da página de detalhes do usuário. | 1 | 1 |
| 20 | GroomMachineMetricDataRetentionDays | MonitorData.Machinemetrics | Essa configuração afeta o gráfico e a tabela na guia "Utilização de Recursos" na página Tendências. | 3 | 3 |
| 21 | GroomMachineMetricDaySummaryDataRetentionDays | MonitorData.MachineMetricDaySummary | Essa configuração afeta o gráfico e a tabela na guia "Utilização | 365 | 31 |

| # | NOME DA CONFIGURAÇÃO | TABELA DE ESQUEMA IMPACTADA | TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR | DIAS DE RETENÇÃO PARA PREMIUM | DIAS DE RETENÇÃO PARA ADVANCED |
|---|---|---|---|---|---|
| | | | de Recursos" na página Tendências. | | |
| 22 | GroomApplicationErrorsRetentionDays | MonitorData.ApplicationError | Esta configuração afeta os detalhes de erro mostrados na coluna "Erros de Aplicativo" na página Aplicativos. | 1 | 1 |
| 23 | GroomApplicationFaultsRetentionDays | MonitorData.Applicationfailure | Esta configuração afeta a coluna "Falhas de Aplicativo" na página Aplicativos. | 1 | 1 |

**Cuidado:**

A modificação de valores no banco de dados do Serviço de Monitoramento requer a reinicialização do serviço para que os novos valores entrem em vigor. É aconselhável fazer alterações no banco de dados do Serviço de Monitoramento somente sob a direção do Suporte Citrix.

> As configurações GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays e GroomSessionMetricsDataRetentionDays são limitadas aos seus valores padrão de 1, enquanto GroomProcessUsageMinuteDataRetentionDays é limitada ao seu valor padrão de 3. Os comandos PowerShell para definir esses valores foram desabilitados, pois os dados de uso do processo tendem a crescer rapidamente. Além disso, as configurações de retenção baseadas em licença são as seguintes:

- **Sites com licença Premium -** a retenção de limpeza para todas as configurações é limitada a 1000 dias (a Citrix recomenda 365 dias).
- **Sites com licença Advanced -** a retenção de limpeza para todas as configurações é limitada a 31 dias.
- **Todos os outros sites -** a retenção de limpeza para todas as configurações é limitada a 7 dias.

**Exceções:**

- GroomApplicationInstanceRetentionDays pode ser definido apenas em sites com licença Premium.
- GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays são limitadas a 31 dias em sites com licença Premium.

Reter dados por longos períodos tem as seguintes implicações no tamanho das tabelas:

- **Dados por hora.** Se os dados por hora puderem permanecer no banco de dados por até dois anos, um site com 1000 grupos de entrega pode fazer com que o banco de dados cresça da seguinte forma:

  1000 grupos de entrega x 24 horas/dia x 365 dias/ano x 2 anos = 17.520.000 linhas de dados. O impacto no desempenho de uma quantidade tão grande de dados nas tabelas de agregação é significativo. Dado que os dados do painel são extraídos desta tabela, os requisitos para o servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto dramático no desempenho.
- **Dados de sessão e evento.** Dados coletados toda vez que uma sessão é iniciada e uma conexão/reconexão é feita. Para um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, o valor de dois anos dessas tabelas coletaria mais de um TB de dados, exigindo um banco de dados de nível empresarial de ponta.

# Motivos de falha e solução de problemas do Citrix Director

As tabelas a seguir descrevem as várias categorias de falha, os motivos e a ação que você precisa tomar para resolver os problemas. Para obter mais informações, consulte Enums, códigos de erro e descrições.

## Erros de falha de conexão

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| N/A | [0] Desconhecido. Este código de erro não está mapeado. | O serviço de Monitoramento não consegue determinar o motivo da falha de inicialização ou conexão relatada a partir das informações compartilhadas pelo serviço de Brokering. | Colete logs CDF no controlador e entre em contato com o suporte da Citrix. |
| [0] Nenhum | [1] Nenhum | Nenhum | N/A |
| [2] Falha da Máquina | [2] Preparação da Sessão | A solicitação de preparação de sessão do controlador de entrega para o VDA falhou. Causas possíveis: Problemas de comunicação entre o controlador e o VDA, problemas encontrados pelo Serviço de Broker ao criar uma solicitação de preparação, ou problemas de rede que resultam na não aceitação da solicitação pelo VDA. | Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com controladores de entrega no Citrix Virtual Apps and Desktops para problemas comuns que causam problemas de comunicação entre o controlador e o VDA. |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| [2] Falha da Máquina | [3] TempoLimiteRegistro | O VDA foi ligado, mas ocorreu um tempo limite enquanto ele tentava se registrar com o controlador de entrega. | Verifique se o Citrix Broker Service está em execução no controlador de entrega e se o serviço Desktop está em execução no VDA. Inicie cada um se estiver parado. |
| [1] Falha na Conexão do Cliente | [4] Tempo Limite de Conexão | O cliente não se conectou ao VDA depois que o VDA foi preparado para o lançamento da sessão. A sessão foi intermediada com sucesso, mas ocorreu um tempo limite enquanto se aguardava a conexão do cliente ao VDA. Causas possíveis: Configurações de firewall, interrupções de rede ou configurações que impedem conexões remotas. | Verifique o console do Director para ver se o cliente tem uma conexão ativa no momento, o que significa que nenhum usuário é afetado. Se nenhuma sessão existir, revise os logs de eventos no cliente e no VDA para quaisquer erros. Resolva quaisquer problemas de conectividade de rede entre o cliente e o VDA. |
| [4] Nenhuma Licença Disponível | [5] Licenciamento | A solicitação de licenciamento falhou. Causas possíveis: Número insuficiente de licenças ou o servidor de licenças está inativo há mais de 30 dias. | Verifique se o servidor de licenças está online e acessível. Resolva quaisquer problemas de conectividade de rede com o servidor de licenças ou reinicie o servidor de licenças se ele |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | parecer estar com mau funcionamento. Verifique se há licenças suficientes no ambiente e aloque mais, se necessário. |
| [1] Falha na Conexão do Cliente | [6] Emissão de Bilhetes | Ocorreu uma falha durante a emissão de bilhetes, indicando que a conexão do cliente com o VDA não corresponde à solicitação intermediada. Um bilhete de solicitação de lançamento é preparado pelo Broker e entregue no arquivo ICA®. Quando o usuário tenta iniciar uma sessão, o VDA valida o bilhete de lançamento no arquivo ICA com o Broker. Causas possíveis: O arquivo ICA está corrompido ou o usuário está tentando fazer uma conexão não autorizada. | Verifique se o usuário tem acesso ao aplicativo ou desktop com base nos grupos de usuários definidos nos grupos de entrega. Instrua o usuário a reiniciar o aplicativo ou desktop para determinar se este é um problema pontual. Se o problema ocorrer novamente, revise os logs de eventos do dispositivo cliente em busca de erros. Verifique se o VDA ao qual o usuário está tentando se conectar está registrado. Se não estiver registrado, revise os logs de eventos no VDA e resolva quaisquer problemas de registro. |
| [1] Falha na Conexão do Cliente | [7] Outro | Uma sessão foi relatada como encerrada pelo VDA | Verifique se a sessão não foi encerrada pelo |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | depois que o cliente contatou inicialmente o VDA, mas antes de concluir a sequência de conexão. | usuário antes do lançamento. Tente relançar a sessão; se o problema persistir, colete os logs CDF e entre em contato com o suporte da Citrix. |
| [1] Falha na Conexão do Cliente | [8] Falha Geral | A sessão falhou ao iniciar. Causas possíveis: Um lançamento intermediado foi solicitado enquanto o intermediador ainda estava iniciando ou inicializando, ou erro interno durante a fase de intermediação de um lançamento. | Verifique se o Serviço de Broker da Citrix está em execução e tente novamente iniciar a sessão. |
| [5] Configuração | [9] Modo de Manutenção | O VDA, ou o grupo de entrega ao qual o VDA pertence, está definido em 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] Configuração | [10] Aplicativo Desabilitado | O aplicativo não pode ser acessado pelos usuários finais porque foi | Se o aplicativo for destinado a uso em produção, habilite o aplicativo e instrua o usuário a reconectar. |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | desabilitado pelo administrador. | |
| [4] Nenhuma Licença Disponível | [11] Recurso de Licença Recusado | O recurso que está sendo usado não é coberto pelas licenças existentes. | Entre em contato com um representante de vendas da Citrix para confirmar os recursos que são cobertos pela edição e tipo de licença existentes do Citrix Virtual Apps and Desktops™. |
| [3] NenhumaCapacidadeDisponível | [13] LimiteDeSessõesAtingido | Todos os VDAs estão em uso e não há capacidade para hospedar mais sessões. Causas possíveis: Todos os VDAs estão em uso (para VDAs de SO de sessão única), ou todos os VDAs atingiram o número máximo configurado de sessões simultâneas permitidas (para VDAs de SO de múltiplas sessões). | Verifique se há VDAs em modo de manutenção. Desative o modo de manutenção se não for necessário para liberar mais capacidade. Considere aumentar o valor de **Número Máximo de Sessões** na configuração da política Citrix para permitir mais sessões por VDA de servidor. Considere adicionar mais VDAs de SO de múltiplas sessões. Considere adicionar mais VDAs de SO de sessão única. |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| [5] Configuração | [14] ProtocoloNãoPermitido | Os protocolos ICA e RDP não são permitidos. | Execute o comando PowerShell **Get-BrokerAccessPolicyRule** no delivery controller e verifique se o valor de **AllowedProtocols** lista todos os protocolos desejados. Este problema ocorre apenas se houver uma configuração incorreta. |
| [5] Configuração | [15] RecursoIndisponível | O aplicativo ou desktop ao qual o usuário está tentando se conectar não está disponível. Este aplicativo ou desktop pode não existir, ou não há VDAs disponíveis para executá-lo. Causas possíveis: O aplicativo ou desktop foi despublicado, ou os VDAs que hospedam o aplicativo ou desktop atingiram a carga máxima, ou o aplicativo ou desktop está configurado em modo de manutenção. | Verifique se o aplicativo ou desktop ainda está publicado e se os VDAs não estão em modo de manutenção. Determine se os VDAs de SO de múltiplas sessões estão com carga total. Se sim, provisione mais VDAs de SO de múltiplas sessões. Verifique se há VDAs de SO de sessão única disponíveis para conexões. Provisione mais VDAs de SO de sessão única, se necessário. |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| [5] Configuração | [16] ActiveSessionReconnectDisabled | A sessão ICA está ativa e conectada a um endpoint diferente. No entanto, como a **Reconexão de Sessão Ativa** está desabilitada, o cliente não consegue se conectar à sessão ativa. | No controlador de entrega, verifique se a **Reconexão de Sessão Ativa** está habilitada. Verifique se o valor de **DisableActiveSessionReconnect** no registro, em **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server**, está definido como 0. |
| [2] MachineFailure | [17] NoSessionToReconnect | O cliente tentou se reconectar a uma sessão específica, mas a sessão foi encerrada. | Tente novamente a reconexão do controle de workspace. |
| [2] MachineFailure | [18] SpinUpFailed | O VDA não pode ser ligado para o lançamento da sessão. Este é um problema relatado pelo hypervisor. | Se a máquina ainda estiver desligada, tente iniciá-la a partir do Citrix Studio. Se isso falhar, revise a conectividade e as permissões do hypervisor. Se o VDA for uma máquina provisionada por PVS, verifique no console do PVS se a máquina está em execução. Caso contrário, verifique se a máquina tem um Personal vDisk atribuído, faça login |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | no hypervisor para redefinir a VM. |
| [2] MachineFailure | [19] Refused | O controlador de entrega envia uma solicitação ao VDA para se preparar para uma conexão de um usuário final, mas o VDA recusa ativamente essa solicitação. | Verifique via ping se o delivery controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas de firewall ou roteamento de rede. |
| [2] Falha da Máquina | [20] Falha de ConfigurationSet | O delivery controller não enviou os dados de configuração necessários, como configurações de política e informações de sessão, para o VDA durante o lançamento da sessão. Causas possíveis: Problemas de comunicação entre o controller e o VDA, problemas encontrados pelo Serviço de Broker ao criar uma solicitação de conjunto de configuração, ou problemas de rede que resultam na não aceitação da solicitação pelo VDA. | - |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| [3] NenhumaCapacidadeDisponível | [21] MaxTotalInstancesExcedido | O número máximo de instâncias de um aplicativo foi atingido. Nenhuma instância adicional do aplicativo pode ser aberta no VDA. Este problema está relacionado ao recurso de limites de aplicativo. | Considere aumentar a configuração do aplicativo, **Limitar o número de instâncias em execução ao mesmo tempo**, para um valor mais alto, se o licenciamento permitir. |
| [3] NenhumaCapacidadeDisponível | [22] MaxPerUserInstancesExcedido | O usuário está tentando abrir mais de uma instância de um aplicativo, mas o aplicativo está configurado para permitir apenas uma única instância do aplicativo por usuário. Este problema está relacionado ao recurso de limites de aplicativo. | Apenas uma instância do aplicativo é permitida por usuário por padrão. Se várias instâncias por usuário forem necessárias, considere desmarcar a configuração **Limitar a uma instância por usuário** na configuração do aplicativo. |
| [1] FalhaDeConexãoDoCliente | [23] Erro de comunicação | O delivery controller tentou enviar informações ao VDA, como uma solicitação para preparar uma conexão, mas ocorreu um erro durante a tentativa de comunicação. Isso pode ser | Se já iniciado, reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verifique se o VDA se registra com sucesso. Confirme se os controladores de entrega configurados para o VDA estão corretos por meio dos |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | causado por interrupções de rede. | detalhes no log de eventos do aplicativo. |
| [3] NoCapacityAvailable | [100] NoMachineAvailable O serviço de monitoramento converte [12] NoDesktopAvailable para este código de erro. | O VDA atribuído para iniciar a sessão está em um estado inválido ou indisponível. Causas possíveis: O estado de energia do VDA é desconhecido ou indisponível, o VDA não reiniciou desde a última sessão do usuário, o compartilhamento de sessão está desabilitado enquanto a sessão atual exige que ele esteja habilitado, ou o VDA foi removido do grupo de entrega ou do site. | Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se há VDAs suficientes registrados e em estado pronto para poder iniciar o desktop compartilhado publicado ou o aplicativo solicitado pelo usuário. Verifique se o hipervisor que hospeda o VDA não está em modo de manutenção. |
| [2] MachineFailure | [101] MachineNotFunctional. O serviço de monitoramento converte [12] NoDesktopAvailable para este código de erro. | O VDA não está operacional. Causas possíveis: O VDA foi removido do grupo de entrega, o VDA está não registrado, o estado de energia do VDA está indisponível, ou o VDA está enfrentando problemas internos. | Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se o VDA aparece como ligado no Citrix Studio. Se o estado de energia for desconhecido para várias máquinas, resolva quaisquer problemas de conectividade com o |

| CATEGORIA | MOTIVO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | hipervisor ou falhas de host. Verifique se o hipervisor que hospeda o VDA não está em modo de manutenção. Reinicie o VDA assim que esses problemas forem resolvidos. |

## Tipo de falha da máquina

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| Desconhecido | - | - | - |
| Não registrado | 3 | - | - |
| MaxCapacity (representado como Carga Máxima no Director) | 4 | A máquina está se reportando com capacidade máxima, ou seja, Índice de Carga Máxima | Certifique-se de que todos os hipervisores estejam ligados. Adicione mais máquinas aos Grupos de Entrega afetados, adicionando mais capacidade ao hipervisor ou adicionando mais hipervisores. |
| StuckOnBoot | 2 | A VM não concluiu sua sequência de inicialização e não está se comunicando com o hipervisor. | Certifique-se de que a VM inicializou com sucesso no hipervisor. Verifique outras mensagens na VM, como problemas de SO. Certifique-se de que |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | as ferramentas do hipervisor estejam instaladas na VM. Certifique-se de que o VDA esteja instalado na VM. |
| FailedToStart | 1 | A VM encontrou problemas ao tentar iniciar no hipervisor. | Verifique os logs do hipervisor. |
| Nenhum | 0 | - | - |

## Motivo do cancelamento de registro da máquina (aplicável quando o tipo de falha é Não Registrado ou Desconhecido)

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| AgentShutdown | 0 | O VDA passou por um desligamento normal. | Ligue o VDA se você não espera que ele esteja desligado com base nas políticas de gerenciamento de energia existentes. Revise quaisquer erros nos logs de eventos. |
| AgentSuspended | 1 | O VDA está em modo de hibernação ou suspensão. | Tire o VDA do modo de hibernação. Considere desabilitar a hibernação para VDAs do Citrix Virtual Apps and Desktops através das configurações de energia. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| IncompatibleVersion | 100 | O VDA não consegue se comunicar com o delivery controller devido a uma incompatibilidade nas versões do protocolo Citrix. | Alinhe as versões do VDA e do delivery controller. |
| AgentAddressResolutionFailed | 101 | O delivery controller não conseguiu resolver o endereço IP do VDA. | Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão corretos. Caso contrário, corrija-os. Se for generalizado, valide as configurações de DNS nos delivery controllers. Verifique a resolução de DNS a partir do controller executando o comando `nslookup`. |
| [Cloud]:AgentAddressResolutionFailed | 101 | O delivery controller não conseguiu resolver o endereço IP do VDA. | Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão corretos. Caso contrário, corrija-os. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| AgentNotContactable | 102 | Ocorreu um problema de comunicação entre o delivery controller e o VDA. | Use um ping para verificar se o delivery controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas de firewall ou rede. Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com delivery controllers no Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controller e o VDA. |
| [Cloud]: AgentNotContactable | 102 | Ocorreu um problema de comunicação entre o delivery controller e o VDA. | Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com delivery controllers no Citrix Virtual Apps and Desktops (CTX136668), para |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | problemas comuns que causam problemas de comunicação entre o controller e o VDA. Entre em contato com o suporte da Citrix. |
| AgentWrongActiveDirectoryOU | 103 | Ocorreu uma configuração incorreta de descoberta do Active Directory. A OU específica do site (onde as informações do site controller são armazenadas no AD) configurada no registro do VDA é para um Site diferente. | Certifique-se de que a configuração do Active Directory esteja correta ou verifique as configurações do registro. |
| EmptyRegistrationRequest | 104 | A solicitação de registro enviada do VDA para o delivery controller estava vazia. Isso pode ser devido a uma instalação de software VDA corrompida. | Reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verifique se o VDA se registra corretamente através do log de eventos do aplicativo. |
| MissingRegistrationCapabilities | 105 | A versão do VDA não é compatível com o delivery controller. | Atualize o VDA ou remova o VDA e reinstale-o. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| MissingAgentVersion | 106 | A versão do VDA não é compatível com o delivery controller. | Reinstale o software VDA se o problema estiver afetando todas as máquinas. |
| InconsistentRegistrationCapabilities | 107 | O VDA não consegue comunicar suas capacidades ao Broker. Isso pode ser devido à incompatibilidade entre as versões do VDA e do delivery controller. As capacidades de registro, que mudam a cada versão, são expressas em um formato que não corresponde à solicitação de registro. | Alinhe as versões do VDA e do delivery controller. |
| NotLicensedForFeature | 108 | O recurso que você está tentando usar não está licenciado. | Verifique sua edição de licenciamento Citrix, ou remova o VDA e reinstale-o. |
| [Cloud]: NotLicensedForFeature | 108 | O recurso que você está tentando usar não está licenciado. | Entre em contato com o suporte da Citrix. |
| Versão de Segurança de Credencial não suportada | 109 | O VDA e o controlador de entrega não estão usando o mesmo mecanismo de criptografia. | Alinhe as versões do VDA e do controlador de entrega. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| InvalidRegistrationRequest | 110 | O VDA fez uma solicitação de registro ao Broker, mas o conteúdo da solicitação está corrompido ou é inválido. | Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com controladores de entrega no Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA. |
| SingleMultiSessionMismatch | 111 | O tipo de sistema operacional do VDA não é compatível com o catálogo de máquinas ou grupo de entrega. | Adicione o VDA ao tipo de catálogo de máquinas ou grupo de entrega correto que contenha máquinas com o mesmo sistema operacional. |
| FunctionalLevelTooLowForCatalog | 112 | O catálogo de máquinas está configurado para um nível funcional de VDA superior à versão do VDA instalada. | Verifique se o nível funcional do catálogo de máquinas do VDA corresponde ao do VDA. Atualize ou faça o downgrade do catálogo de máquinas para corresponder ao do VDA. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| FunctionalLevelTooLowForDesktopGroup | 113 | O grupo de entrega está configurado para um nível funcional de VDA superior à versão do VDA instalada. | Verifique se o nível funcional do grupo de entrega do VDA corresponde ao do VDA. Atualize ou faça o downgrade do catálogo de máquinas para corresponder ao do VDA. |
| PowerOff | 200 | O VDA não foi desligado corretamente. | Se o VDA deveria estar ligado, tente iniciar o VDA a partir do Citrix Studio e verifique se ele inicializa e se registra corretamente. Solucione quaisquer problemas de inicialização ou registro. Revise os logs de eventos no VDA assim que ele estiver novamente online para ajudar a determinar a causa raiz do desligamento. |
| AgentRejectedSettingsUpdate | 203 | Configurações como políticas Citrix foram alteradas ou atualizadas, mas houve um erro ao enviar as atualizações para o VDA. Isso pode ocorrer se as | Atualize o VDA se necessário. Verifique se as atualizações aplicadas são compatíveis com a versão do VDA. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | atualizações forem incompatíveis com a versão do VDA instalada. | |
| SessionPrepareFailure | 206 | O Broker não concluiu uma auditoria das sessões em execução no VDA. | Se for generalizado, reinicie o Citrix Broker Service no delivery controller. |
| [Cloud]: SessionPrepareFailure | 206 | O Broker não concluiu uma auditoria das sessões em execução no VDA. | Entre em contato com o suporte da Citrix. |
| ContactLost | 207 | O delivery controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções de rede. | Verifique se o Citrix Broker Service está em execução no delivery controller e se o serviço Desktop está em execução no VDA. Inicie cada um se estiverem parados. Se já estiverem iniciados, reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verifique se o VDA se registra com sucesso. Confirme se os delivery controllers configurados para o VDA estão corretos por meio dos detalhes no log de |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | eventos do Aplicativo. Use um ping para verificar se o delivery controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas de firewall ou rede. |
| [Cloud]: ContactLost | 207 | O delivery controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções de rede. | Verifique se o serviço Desktop está em execução no VDA. Inicie-o se estiver parado. |
| BrokerRegistrationLimitReached | 301 | O delivery controller atingiu o número máximo configurado de VDAs que podem se registrar simultaneamente. Por padrão, o delivery controller permite 10.000 registros simultâneos de VDA. | Considere adicionar delivery controllers ao Site ou criar um Site. Você também pode aumentar o número de VDAs permitidos para se registrar simultaneamente com o delivery controller através da chave de registro **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers**. Consulte o artigo da Central de Conhecimento, Entradas de Chave de Registro Usadas pelo Citrix Virtual |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | | Apps and Desktops (CTX117446) para obter mais informações. Aumentar esse número pode exigir mais recursos de CPU e memória para o controller. |
| SettingsCreationFailure | 208 | O Broker não construiu um conjunto de configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falhará e o VDA ficará não registrado. | Verifique os logs de eventos no delivery controller em busca de erros. Reinicie o Serviço Broker se um problema específico não for evidente nos logs. Assim que o Serviço Broker for reiniciado, reinicie o serviço Desktop nos VDAs afetados e verifique se eles se registram com sucesso. |
| [Cloud]: SettingsCreationFailure | 208 | O Broker não construiu um conjunto de configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falhará e o VDA ficará não registrado. | Reinicie o serviço Desktop nos VDAs afetados e verifique se eles se registram com sucesso. Entre em contato com o suporte da Citrix. |
| SendSettingsFailure | 204 | O Broker não enviou as configurações e os dados de | Se limitado a um único VDA, reinicie o serviço Desktop no |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| | | configuração para o VDA. Se o Broker puder coletar os dados, mas não conseguir enviá-los, o registro falhará. | VDA para forçar o novo registro e valide se o VDA se registra com sucesso através do log de eventos do aplicativo. Solucione quaisquer erros observados. Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com controladores de entrega no Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA. |
| AgentRequested | 2 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |
| DesktopRestart | 201 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |
| DesktopRemoved | 202 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |

| CÓDIGO DE ERRO | ID DO CÓDIGO DE ERRO | PROBLEMA | AÇÃO |
|---|---|---|---|
| SessionAuditFailure | 205 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |
| UnknownError | 300 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |
| RegistrationStateMismatch | 302 | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |
| Desconhecido | - | Ocorreu um erro desconhecido. | Entre em contato com o suporte da Citrix. |

# Integração do Secure Private Access com o Director (Prévia)

A integração do Secure Private Access com o Director permite que o administrador do help desk ou o administrador completo monitore e solucione problemas de todas as sessões do Secure Private Access no Director. Para oferecer suporte a esse recurso, você deve usar as versões 2402 ou posteriores do Director, Secure Private Access, aplicativo Citrix Workspace™ e VDA.

As ações disponíveis incluem a visualização dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário no pop-up **Selecionar uma Sessão** > guia **Sessões** > **Aplicativos Web e Aplicativos SaaS**
- Enumerações falhas ou bloqueadas do Secure Private Access e inicializações de aplicativos falhas no pop-up **Selecionar uma Sessão** > guia **Acesso Negado**
- Visualização de detalhes da sessão e do aplicativo para inicializações de aplicativos ativas e falhas
- Visualização de detalhes da sessão e do aplicativo para enumerações falhas e bloqueadas

**Nota:**

> A integração do Secure Private Access com o Director é suportada apenas para autenticação baseada em formulários do Director e não é suportada para Autenticação Integrada do Windows ou autenticação baseada em Smart Card.

## Pré-requisitos

1. Para oferecer suporte a esse recurso, você deve usar o seguinte:
   - Director 2402 ou versão posterior
   - Secure Private Access 2402 ou versão posterior
   - Aplicativo Citrix Workspace 2402 ou versão posterior
2. Certifique-se de que pelo menos um site do Citrix Virtual Apps and Desktops™ esteja configurado no Director.
3. Configurar o Secure Private Access.
4. Certifique-se de que o servidor Director tenha conectividade de rede com o servidor Secure Private Access.

   > **Nota:**
   >
   > Um certificado confiável deve ser instalado no servidor Secure Private Access para estabelecer uma conexão bem-sucedida com o Citrix Director.

5. Certifique-se de que o usuário administrador do Director tenha as seguintes permissões:
   a. Administrador Completo do Secure Private Access ou Administrador Somente Leitura no console de administração do Secure Private Access.
   b. Help desk do Citrix Virtual Apps™ ou Desktops ou Administrador Completo ou Administrador Somente Leitura no console do Citrix Studio.

## Configurar o Director com o Secure Private Access

1. Abra um prompt de comando como administrador na máquina onde o Director está instalado.
2. Vá para o caminho da ferramenta `DirectorConfig` executando o seguinte comando:

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Execute o seguinte comando para configurar o Secure Private Access:

```
DirectorConfig.exe /configspa
```

4. Insira o FQDN da máquina onde o Secure Private Access está instalado, juntamente com o número da porta.
5. Certifique-se de que a conexão com o Secure Private Access (servidor ou balanceador de carga) seja segura e tenha um certificado confiável aplicado a ela.

```
PS C:\inetpub\wwwroot\Director\tools> .\DirectorConfig.exe /configspa

 Make sure the SPA server or load balancer is reachable from this Director machine
 Enter SPA server or load balancer FQDN including port [https://spa-server.mydomain.com:4443] : https://spa1.gwonprem.corp:4443

 Checking connectivity to https://spa1.gwonprem.corp:4443

 Spa Server or load balancer: https://spa1.gwonprem.corp:4443 is reachable.

 Checking Spa Server or load balancer is valid

 Retry with correct Spa Server FQDN which is reachable

 Director configuration encountered an error


=====================================================
Spa Server or load balancer FQDN https://spa1.gwonprem.corp:4443 is either invalid or Spa server/load balancer is down
=====================================================
```

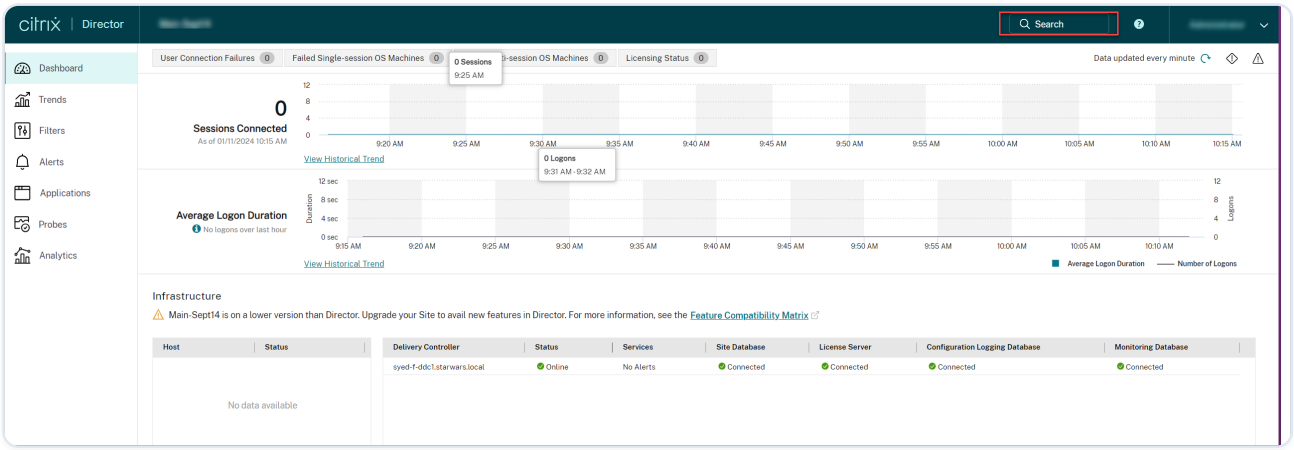
**Nota:**

Os administradores devem ser adicionados ao console do Secure Private Access para visualizar os detalhes da sessão do Secure Private Access no Director. Para obter mais informações, consulte Gerenciar administradores.

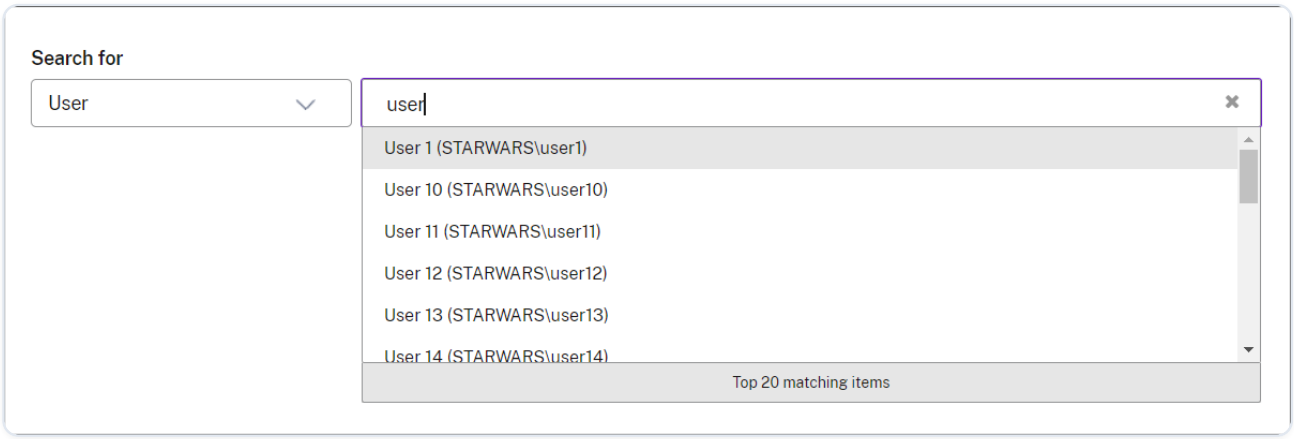
## Visualizar uma sessão do Secure Private Access por usuário

No painel do Director, clique em **Pesquisar** e insira o nome de usuário. A tela **Selecionar uma sessão** é exibida.

**Administrador completo:**

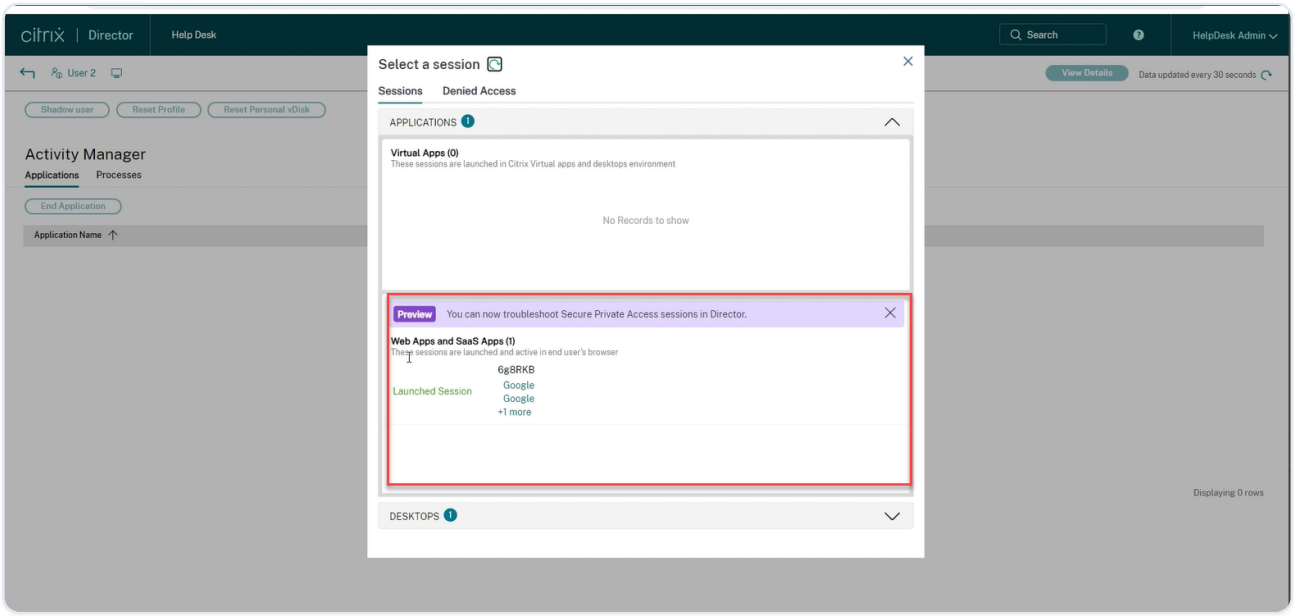



**Administrador de help desk:**

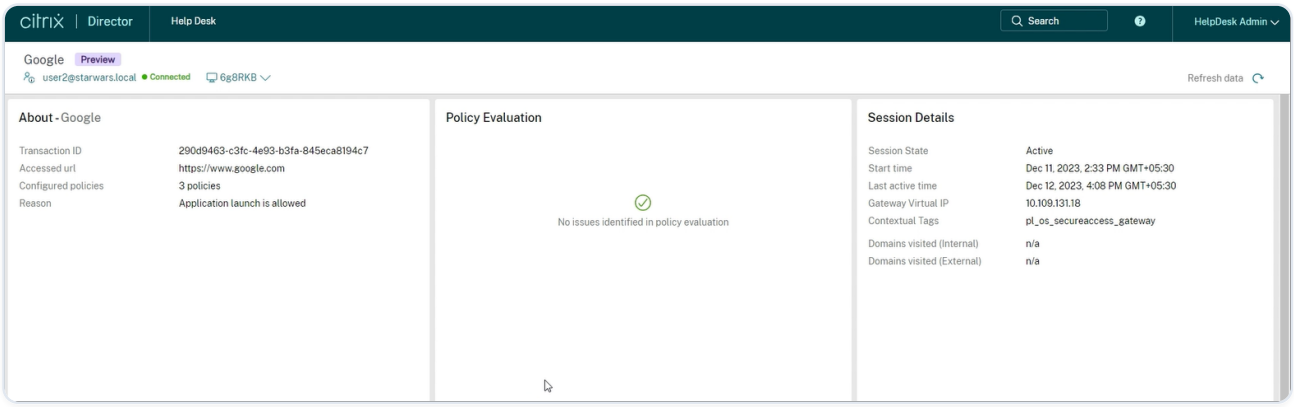



# Visualizar aplicativos Web e SaaS iniciados com sucesso

Os aplicativos iniciados com sucesso são exibidos na seção **Aplicativos Web e SaaS**.



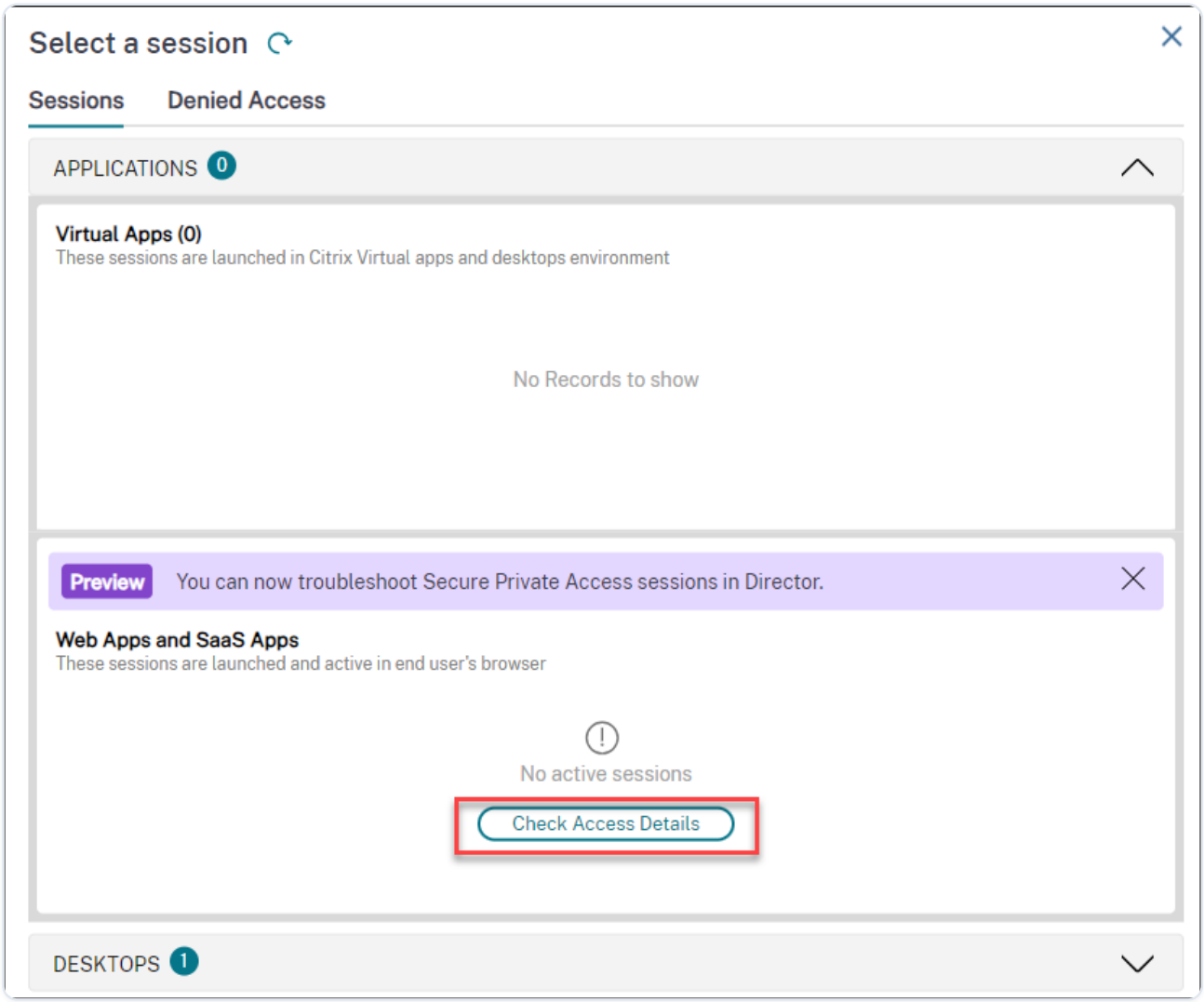

Clique em um aplicativo na seção **Aplicativos Web e SaaS** para visualizar os detalhes.




Para obter mais informações sobre códigos de sucesso, consulte Códigos relacionados ao Citrix Director.

## Visualizar detalhes sobre os aplicativos com acesso negado

Clique em **Verificar Detalhes de Acesso** na tela **Selecionar uma sessão**.



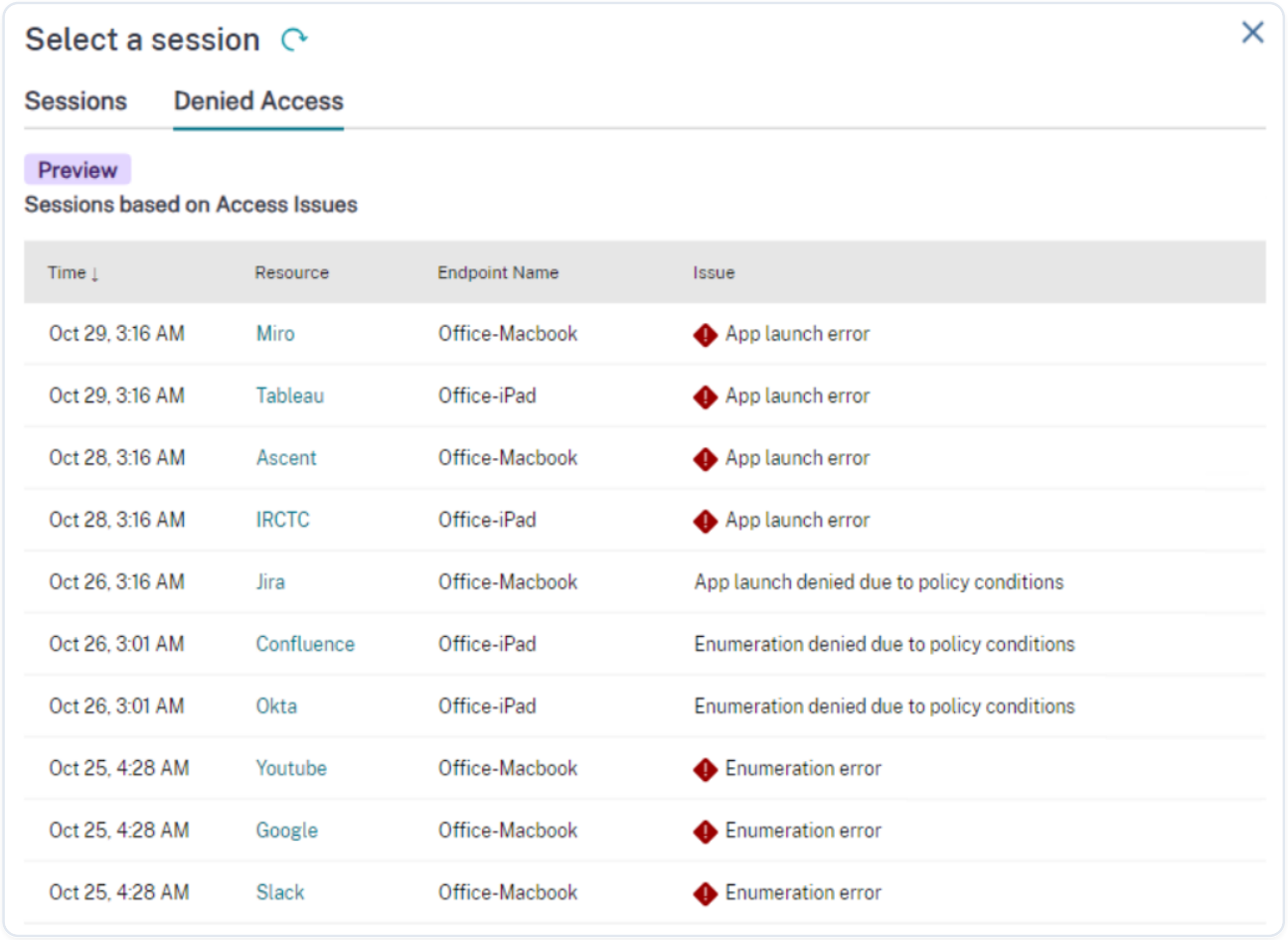

**Nota:**

> O botão **Verificar Detalhes de Acesso** aparece quando não há sessão ativa.

> Ou,

Clique na guia **Acesso Negado** para visualizar os aplicativos para os quais o acesso foi negado.

A guia **Acesso Negado** é aberta.

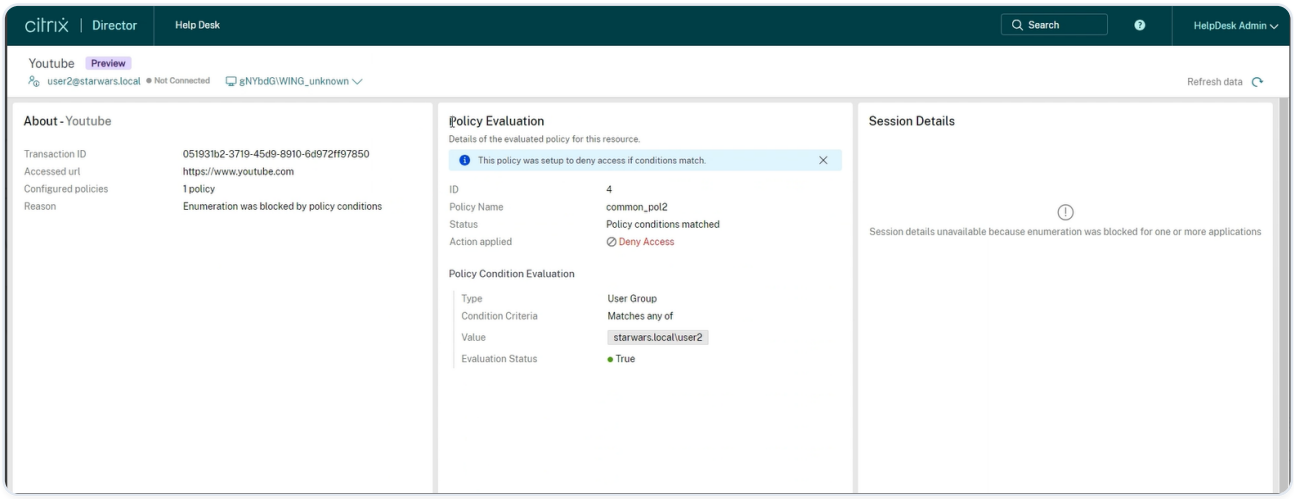



Os detalhes da sessão, como hora, recurso, nome do endpoint e motivo da falha, são exibidos. Para obter mais informações sobre códigos de erro, consulte Códigos relacionados ao Citrix Director.

Atualmente, os seguintes problemas foram identificados:

- Enumeração negada devido às condições da política
- Erro de inicialização do aplicativo
- Erros de enumeração
- Inicialização do aplicativo negada devido às condições da política

Selecione um aplicativo na guia **Acesso Negado** > coluna **Recurso** para visualizar os detalhes:




Os seguintes detalhes são exibidos para as sessões bem-sucedidas ou com falha:

- Sobre o aplicativo
- Avaliação da política
- Detalhes da sessão

### Sobre o aplicativo

O nome do aplicativo bem-sucedido, com falha ou negado é exibido. Junto com ele, os seguintes detalhes do aplicativo para o sucesso ou falha são exibidos:

| CAMPO | DESCRIÇÃO |
|---|---|
| ID da Transação | ID de transação Citrix durante a sessão ou enumeração. |
| URL acessada | A URL acessada durante a sessão ou enumeração. |
| Políticas configuradas | O número de políticas que são usadas em uma sessão ou enumeração. |
| Motivo | A análise da sessão ou da atividade de enumeração. |

### Avaliação da política

Exibe que nenhum problema foi encontrado durante a avaliação de uma sessão bem-sucedida. Para uma sessão ou enumeração com falha, os seguintes detalhes das políticas avaliadas são exibidos:

| CAMPO | DESCRIÇÃO |
|---|---|
| ID | ID de Transação Citrix. |
| Nome da Política | O nome da política. |
| Status | O status da política. |
| Ação aplicada | A ação aplicada à política. Por exemplo, negar acesso. |
| Avaliação da Condição da Política | |
| Tipo | O tipo da condição da política. |
| Critérios da Condição | Os critérios de condição da política aplicada na sessão ou enumeração com falha. |
| Valor | O valor da política. |
| Status da Avaliação | O status de avaliação da política. |

### Detalhes da sessão

Para uma sessão com falha, o motivo da falha da sessão é exibido. Para uma sessão bem-sucedida, os seguintes detalhes são exibidos:

| CAMPO | DESCRIÇÃO |
|---|---|
| Estado da Sessão | Exibe o estado da sessão, seja ela ativa ou inativa. |
| Hora de início | Exibe a hora de início da sessão. |
| Última hora ativa | Exibe a última hora ativa da sessão bem-sucedida. |
| IP Virtual do Gateway | Exibe o endereço IP virtual do gateway ao qual a sessão bem-sucedida está conectada. |
| Tags Contextuais | Exibe as tags contextuais. A tag contextual no plug-in do Secure Private Access é o nome de uma política do NetScaler® Gateway (sessão, |

| CAMPO | DESCRIÇÃO |
| --- | --- |
| | pré-autenticação, EPA) que é aplicada às sessões dos usuários autenticados. |
| Domínios visitados (Internos) | Exibe os domínios internos acessados usando a sessão bem-sucedida. |
| Domínios visitados (Externos) | Exibe os domínios externos acessados usando a sessão bem-sucedida. |

# SDKs e APIs

Vários SDKs e APIs estão disponíveis com esta versão. Para acessar os SDKs e APIs, vá para Crie qualquer coisa com Citrix. A partir daí, selecione **Citrix Workspace** para acessar informações de programação para Citrix Virtual Apps and Desktops e seus componentes relacionados.

> **Nota:**
>
> O SDK do Citrix Virtual Apps and Desktops™ e o SDK do Citrix Group Policy podem ser instalados como um módulo ou um snap-in. Vários SDKs de componentes (como Citrix Licensing, Citrix Provisioning e StoreFront) são instalados usando apenas um snap-in.

> Este produto suporta as versões 3 a 5 do PowerShell.

## SDK do Citrix Virtual Apps and Desktops

Este SDK é instalado automaticamente como um módulo do PowerShell quando você instala um Delivery Controller™ ou o Studio. Isso permite que você use os cmdlets deste SDK sem precisar adicionar snap-ins. (As instruções são fornecidas abaixo se você optar por instalar este SDK como um snap-in.)

### Permissões

Você deve executar o shell ou script usando uma identidade que tenha direitos de administração Citrix. Embora os membros do grupo de administradores locais no Controller tenham automaticamente privilégios administrativos completos para permitir a instalação do Citrix Virtual Apps ou Citrix Virtual Desktops™, a Citrix recomenda que, para operação normal, você crie administradores Citrix com os direitos apropriados, em vez de usar a conta de administradores locais.

### Acessar e executar os cmdlets

1. Iniciar um shell no PowerShell: Abra o Studio, selecione a guia **PowerShell** e clique em **Launch PowerShell**.

2. Para usar cmdlets do SDK em scripts, defina a política de execução no PowerShell. Para obter informações sobre a política de execução do PowerShell, consulte a documentação da Microsoft.
3. Se você quiser usar o snap-in (em vez do módulo), adicione o snap-in usando o cmdlet `Add-PSSnapin` (ou `asnp`).

   V1 e V2 denotam a versão do snap-in. Os snap-ins do XenDesktop 5 são a versão 1. Citrix Virtual Apps and Desktops, e os snap-ins de versões anteriores do XenDesktop 7 são a versão 2. Por exemplo, para instalar o snap-in do Citrix Virtual Apps and Desktops, digite `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Para importar todos os cmdlets, digite: `Add-PSSnapin Citrix.*.Admin.V*`

Agora você pode usar os cmdlets e os arquivos de ajuda.

- Para acessar os arquivos de ajuda para este SDK, selecione o produto ou componente na lista Categorias, e então selecione **Citrix Virtual Apps and Desktops SDK**.
- Para orientação sobre PowerShell, consulte Windows PowerShell Integrated Scripting Environment (ISE).

# SDK do Group Policy

O SDK do Citrix Group Policy permite exibir e configurar as configurações e filtros do Group Policy. Este SDK usa um provedor do PowerShell para criar uma unidade virtual que corresponde às configurações e filtros da máquina e do usuário. O provedor aparece como uma extensão para `New-PSDrive`.

Para usar o SDK do Group Policy, o Studio ou o SDK do Citrix Virtual Apps and Desktops deve estar instalado.

O provedor PowerShell de Política de Grupo Citrix está disponível como um módulo ou um snap-in.

- Para usar o módulo, nenhum trabalho adicional é necessário.
- Para adicionar o snap-in, digite `Add-PSSnapin citrix.common.grouppolicy`.

Para acessar a ajuda, digite: `help New-PSDrive -path localgpo:/`.

Para criar uma unidade virtual e carregá-la com configurações, digite `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` onde a string do

Controller é o nome de domínio totalmente qualificado de um Controller no site ao qual você deseja se conectar e carregar as configurações.

## APIs REST do Citrix Virtual Apps and Desktops

Com as APIs REST do Citrix Virtual Apps and Desktops, você pode automatizar o gerenciamento de recursos em uma implantação do Citrix Virtual Apps and Desktops.

As APIs REST do Citrix Virtual Apps and Desktops estão disponíveis em `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>`. As APIs não aplicáveis ao Citrix Virtual Apps and Desktops são marcadas de acordo. Siga as orientações para configurar o acesso ao serviço de API e usar as APIs para gerenciar e otimizar seus recursos.

## OData do Serviço de Monitoramento

A API Monitor permite o acesso aos dados do Serviço de Monitoramento usando a Versão 3 ou 4 da API OData. Você pode criar painéis de monitoramento e relatórios personalizados com base nos dados consultados do Serviço de Monitoramento. O OData V.4 é baseado na API Web ASP.NET e oferece suporte a consultas de agregação.

Para obter mais informações, consulte a API OData do Serviço Monitor.

# __index__

## Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site.

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar pelos gráficos de tendências, ampliando um período de tempo (clicando em um ponto de dados no gráfico) e detalhando para ver os detalhes associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que é afetado.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

Escolha um período de tempo para o qual você precisa das informações de tendências históricas. A disponibilidade do período de tempo depende da sua implantação do Director da seguinte forma:

- Relatórios de tendências de até o Último ano (365 dias) estão disponíveis em sites com licença Premium.
- Relatórios de tendências de até o Último mês (31 dias) estão disponíveis em sites com licença Advanced.

- Relatórios de tendências de até os Últimos 7 dias em sites sem licença Premium e sem licença Advanced.

**Nota:**

- Em todas as implantações do Director, as informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Último mês (**Terminando agora**) ou menor. Para o período escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendência estão disponíveis como gráficos e não como tabelas.
- Os valores de retenção de limpeza do Serviço de Monitoramento controlam a disponibilidade dos dados de tendências. Os valores padrão estão disponíveis em Granularidade e retenção de dados. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção.
- Os seguintes parâmetros no Gerenciador do IIS controlam o intervalo de datas de término personalizadas disponíveis para seleção. No entanto, a disponibilidade dos dados para as datas selecionadas depende da configuração de retenção de limpeza para a métrica específica que está sendo medida.

| PARÂMETRO | VALORES PADRÃO |
|---|---|
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

## Tendências disponíveis

**Visualizar tendências para sessões:** Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é habilitada quando as políticas de Confiabilidade da

Sessão ou Reconexão Automática do Cliente estão em vigor. Quando há uma interrupção de rede no endpoint, as seguintes políticas entram em vigor:

- A confiabilidade da sessão entra em vigor (por padrão por 3 minutos) onde o Citrix Receiver™ ou o aplicativo Citrix Workspace™ tenta se conectar ao VDA.
- A reconexão automática do cliente entra em vigor entre 3 e 5 minutos, onde o cliente tenta se conectar ao VDA.

Ambas as reconexões são capturadas e exibidas ao usuário. Esta informação pode levar um tempo máximo de 5 minutos para aparecer na interface do usuário do Director após a reconexão ter ocorrido.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções. Também analisa redes com uma experiência contínua. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período selecionado nos Filtros. Um detalhamento fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Este recurso requer Delivery Controller™ versão 7 1906 ou posterior, e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações da política de reconexão automática do cliente e Configurações da política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Director pelos seguintes motivos:

- O aplicativo Workspace não está enviando dados de reconexão automática para o VDA.
- O VDA não está enviando dados para o serviço de monitoramento.
- Os Delivery Controllers descartam cargas úteis de VDA, pois podem não ter as sessões correspondentes.

> **Nota:**

> Às vezes, o endereço IP do cliente pode não ser obtido corretamente se certas políticas do Citrix Gateway estiverem definidas.

> **Visualizar tendências de falhas de conexão:** Na guia Falhas, selecione a conexão, o tipo de máquina, o tipo de falha, o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em seu site.

**Visualizar tendências de falhas de máquina:** Na guia **Falhas de Máquina de SO de Sessão Única** ou na guia Máquinas de SO de Múltiplas Sessões, selecione o tipo de falha, o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de máquina em seu site.

**Visualizar tendências de desempenho de logon:** Na guia **Desempenho de Logon**, selecione o Grupo de Entrega e o período para visualizar um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em seu site e se o número de logons afeta o desempenho. Esta exibição também mostra a duração média das fases de logon, como duração de corretagem e tempo de inicialização da VM. Esses dados são especificamente para logons de usuário e não incluem usuários tentando se reconectar de sessões desconectadas. A tabela abaixo do gráfico mostra a Duração do Logon por Sessão do Usuário. Você pode escolher as colunas a serem exibidas e classificar o relatório por qualquer uma das colunas. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

**Visualizar tendências de avaliação de carga:** Na guia **Índice do Avaliador de Carga**, visualize um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas de SO de Múltiplas Sessões. As opções de filtro para este gráfico incluem o Grupo de Entrega ou a máquina de SO de Múltiplas Sessões em um Grupo de Entrega, a máquina de SO de Múltiplas Sessões (disponível apenas se a máquina de SO de Múltiplas Sessões em um Grupo de Entrega foi selecionada) e o intervalo.

**Visualizar uso de aplicativos hospedados:** A disponibilidade desse recurso depende da licença da sua organização. Na guia **Gerenciamento de Capacidade**, selecione a guia **Uso de Aplicativos Hospedados**. Selecione o Grupo de Entrega e o período para visualizar um gráfico exibindo o pico de uso simultâneo e uma tabela exibindo o uso baseado em aplicativo. Na tabela Uso Baseado em Aplicativo, você pode escolher um aplicativo específico para ver detalhes e uma lista de usuários que estão usando ou usaram o aplicativo.

**Visualizar uso de SO de Sessão Única e Múltiplas Sessões:** A exibição Tendências mostra o uso de SO de Sessão Única por site e por Grupo de Entrega. Ao selecionar **Site**, o uso é mostrado por Grupo de Entrega. Ao selecionar Grupo de Entrega, o uso é mostrado por Usuário. A

exibição Tendências também mostra o uso de SO de Múltiplas Sessões por site, por Grupo de Entrega e por Máquina. Ao selecionar **Site**, o uso é mostrado por Grupo de Entrega. Ao selecionar Grupo de Entrega, o uso é mostrado por Máquina e por Usuário. Quando Máquina é selecionada, o uso é mostrado por Usuário.

**Visualizar uso de máquina virtual:** Na guia **Uso da Máquina**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter uma visualização em tempo real do uso da sua VM, permitindo que você avalie rapidamente as necessidades de capacidade do seu site. Disponibilidade de SO de Sessão Única - exibe o estado atual das máquinas de SO de Sessão Única (VDIs) por disponibilidade para todo o site ou um Grupo de Entrega específico. Disponibilidade de SO de Múltiplas Sessões - exibe o estado atual das máquinas de SO de Múltiplas Sessões por disponibilidade para todo o site ou um Grupo de Entrega específico.

> **Nota:** O número de máquinas exibidas no Contador Disponível inclui máquinas em modo de manutenção.

> **Visualizar utilização de recursos:** Na guia **Utilização de Recursos**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter informações sobre dados de tendências históricas para uso de CPU e memória, e IOPS e latência de disco para cada máquina VDI para um melhor planejamento de capacidade. Este recurso requer Delivery Controllers e VDAs **versão 7.11** ou posterior. Os gráficos mostram dados para CPU média, memória média, IOPS médio, latência de disco e pico de sessões simultâneas. Você pode detalhar a máquina e visualizar dados e gráficos para os 10 principais processos que consomem CPU.

Filtre por Grupo de Entrega e Período. Os gráficos de uso de CPU, memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, mês e ano. Os gráficos de IOPS médio e latência de disco estão disponíveis para as últimas 24 horas, mês e ano.

> **Nota:**
>
> - A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como **Permitido** para coletar e exibir dados na tabela dos 10 Principais Processos na página Utilização Histórica da Máquina. A política é definida como **Proibido** por padrão. Todos os dados de utilização de recursos são coletados por

padrão. Isso pode ser desabilitado usando a configuração da política **Habilitar Monitoramento de Recursos**. A tabela abaixo dos gráficos mostra os dados de utilização de recursos por máquina. Para obter mais informações, consulte Configurações da política de monitoramento.

- O IOPS médio mostra as médias diárias. O IOPS de pico é calculado como o maior das médias de IOPS para o intervalo de tempo selecionado. (Uma média de IOPS é a média horária de IOPS coletados durante a hora no VDA).
- O detalhamento da máquina lista processos com uso médio de CPU ou memória média superior a 1%, o que pode significar que, às vezes, menos de 10 processos são listados.

**Visualizar dados de análise de rede:** A disponibilidade desse recurso depende da licença da sua organização e das suas permissões de administrador. Este recurso requer Delivery Controllers **versão 7.11** ou posterior.

Na guia **Rede**, monitore sua análise de rede, que fornece uma visão contextual da rede para usuário, aplicativo e desktop. Com esse recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação por meio de relatórios HDX Insight do Citrix ADM. Para obter mais informações, consulte Configurar análise de rede

**Exibir falhas de aplicativo:** A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de várias sessões executando Windows Server 2008 e posterior são suportados. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas falhas de aplicativo de VDAs de SO de várias sessões são exibidas. Você pode definir o monitoramento de falhas de aplicativo usando políticas de Monitoramento. Para obter mais informações, consulte Configurações de política de monitoramento.

**Exibir resultados da sondagem:** A guia **Resultados da Sondagem** exibe os resultados da sondagem para aplicativos e desktops que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha ocorreu é registrado.

Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

**Criar relatórios personalizados:** A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados históricos e em tempo real do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatório Personalizado salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique condições de filtro com base em campos como máquina, Grupo de Entrega ou período de tempo. Especifique colunas adicionais necessárias em seu Relatório Personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta de Relatório Personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta de Relatório Personalizado com base em uma consulta OData copiada. Para fazer isso, selecione a opção Consulta OData e cole a consulta OData copiada. Você pode salvar a consulta resultante para execução posterior.

> **Nota:** Os nomes das colunas nos relatórios de Visualização e Exportação gerados usando consultas OData não são localizados, mas aparecem em inglês.

> Os ícones de bandeira no gráfico indicam eventos ou ações significativas para aquele intervalo de tempo específico. Passe o mouse sobre a bandeira e clique para listar eventos ou ações.

> **Nota:**
>
> - Os dados de logon de conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
> - Grupos de Entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros de Tendências do Director até que os dados relacionados a eles sejam removidos. A seleção de um Grupo de Entrega excluído exibe gráficos para os dados disponíveis até a retenção. No entanto, as tabelas não mostram dados.

- Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro faz com que as tabelas **Utilização de Recursos e Índice do Avaliador de Carga** do novo Grupo de Entrega exibam métricas consolidadas dos Grupos de Entrega antigo e novo.