Citrix Aplicativos Virtuais e Áreas de Trabalho™ 7 2203 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 para qualquer dispositivo, em qualquer rede, ao mesmo tempo em que aprimora a segurança dos dados, reduz custos e aumenta a produtividade.

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

A Atualização Cumulativa 6 (CU6) é a atualização mais recente para o LTSR 2203. LTSRs também estão disponíveis para Citrix Virtual Apps and Desktops 1912 e XenApp e XenDesktop Versão 7.15.

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

Versões anteriores

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

Para versões ainda mais antigas, a documentação está 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
- Perguntas Frequentes do LTSR
- Opções de serviço do Citrix Virtual Apps and Desktops
- Datas do ciclo de vida do produto
- Programa LTSR para Citrix Workspace app
- Descontinuações

Novidades

Atualização Cumulativa 7 (CU7)

Data de lançamento: Aug 28, 2025

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 7 (CU7) corrige mais de 25 problemas relatados desde o lançamento do 2203 LTSR CU5.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

O que há de novo nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU5

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Aplicativos Virtuais e Desktops 7 2203 LTSR CU7

Novas implantações

Como faço para implantar o CU7 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU7 - usando o metainstalador do CU7. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Examine a seção Citrix Virtual Apps and Desktops 7 2203 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 CU7 fornece atualizações para 15 componentes de linha de base do 2203 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU7. 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 2203 LTSR CU7

COMPONENTE DE LINHA DE BASE DO 2203 CU7	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.7000.7522	VDA de sessão única
VDA de múltiplas sessões	2203.0.7000.7522	VDA de múltiplas sessões
Delivery Controller	2203.0.7000.7522	Delivery Controller(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller)
Citrix Studio	7.33.7000.57	Citrix Studio(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#citrix-studio)
Citrix Director	7.33.7000.26	Citrix Director(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/director.html)
Citrix Group Policy Management	7.33.7000.20	Citrix Group Policy Management(/pt-br/citrix-virtual-apps-desktops/2203-

COMPONENTE DE LINHA DE BASE DO 2203 CU7	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
		ltsr/policies/policies-processes.html)
Citrix Group Policy Client-Side Extension	7.33.7000.16	
Citrix StoreFront	2203.0.7000.7	Citrix StoreFront(/pt-br/storefront/)
Citrix Provisioning	7.33.40	Citrix Provisioning
Servidor de Impressão Universal	7.33.7000.18	Universal Print Server
Gravação de Sessão	22.3.7000	Session Recording
Linux VDA	22.03.6000	Linux Virtual Delivery Agent
Gerenciamento de Perfis	22.3.7000.10	Profile Management
Citrix Federated Authentication Service	10.9.700.16	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.32.7000.10	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2305	2305.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU7

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 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2309	Citrix App Layering
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Servidor de Licenças	11.17.2.0_BUILD_53100	Servidor de Licenças
Camada de personalização do usuário	25.3.3	Camada de personalização do usuário
Reprodutor web de Gravação de Sessão	22.3.7000.6	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32.3000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	22.12.0	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa mais recente	Documentação

2203 LTSR CU7 exclusões notáveis

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. 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
Framehawk

COMPONENTES E RECURSOS EXCLUÍDOS
Personal vDisk
StoreFront Citrix Online Integration
License Activation Service

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 2203 LTSR Cumulative Update 7 (CU7).

> **Observação:**

> Se você estiver no 2203 LTSR CU7, recomendamos 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 recomendado 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 de Vida (EOL) em April 15, 2026. O 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 suportado, 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.

Delivery Controller

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

Para criação e atualizações de sites 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 2203 LTSR CU6:

Delivery Controller™

- A limpeza do Monitor Service pode falhar devido a um nome de variável inválido na definição da tarefa. Esse problema afeta a tarefa `GroomResourceUtilization` e também pode impactar outras tarefas de limpeza.
- 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%
- Você pode não conseguir criar um novo catálogo de máquinas ou ligar VDAs existentes após atualizar do 1912 CU8 para o 2203 CU4 ao usar um símbolo decimal não padrão como ','
- A atualização de um Delivery Controller do 2203 CU5 para o 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 termina com sucesso.

Gráficos

- 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.
- 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".

Metainstalador

- Após a atualização para o VDA 2203, a primeira sessão ICA após uma reinicialização não é iniciada. Você pode resolver isso iniciando a sessão uma segunda vez.
- A atualização do VDA do 2203 CU3 para o 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, pode ser necessário reaplicá-las após a atualização.

Servidor de Impressão Universal

Impressão

- Após a atualização do Universal Print Server (UPS) para o 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

- Depois de iniciar a sessão, conectar e desconectar o dispositivo de áudio várias vezes faz com que a sessão pare de reconhecer o dispositivo de áudio.
- Você pode encontrar um erro de tela azul com um código de parada durante o desligamento.

Exceções do Sistema

- Ao usar o Windows 11 24H2, a sessão trava e exibe uma tela preta durante a inicialização.
- Após a atualização para VDA 2203 CU5 ou CU6, você pode não conseguir fazer login em servidores, as sessões param de responder durante o logon ou logoff.
- 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.

- No CVAD 2203 CU5, seu dispositivo pode exibir um erro de tela azul devido a um novo problema com o picadm.sys.
- 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.

VDA para SO multissessão

Área de Transferência

- Ao usar o Citrix Workspace™ para HTML5, a sessão trava depois de copiar e colar grandes quantidades de dados no Excel.
- 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 da área de transferência devido a um problema na DLL da Área de Transferência.

Sessão/Conexão

- 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.
- 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.
- Você pode encontrar um erro de tela azul com um código de parada durante o desligamento.
- Ao iniciar sessões do Citrix Workspace App para Linux, as sessões parecem abrir, mas fecham imediatamente sem mostrar nenhum erro.

Exceções do Sistema

- Após a atualização para VDA 2203 CU5 ou CU6, você pode não conseguir fazer login em servidores, as sessões param de responder durante o logon ou logoff.
- 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.
- No CVAD 2203 CU5, seu dispositivo pode exibir um erro de tela azul devido a um novo problema com picadm.sys.
- 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.

- Depois de atualizar para 2203 CU5 VDA, a sessão não fecha após você sair do aplicativo.
- O LastPingTime não é atualizado no registro com 2203 CU5, o que pode fazer com que você seja desconectado.
- Você pode experimentar falhas aleatórias com um código de verificação de bug indicando um problema de driver.
- 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.

Citrix Provisioning™

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

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.

Atualização Cumulativa 6 (CU6)

Data de lançamento: Jan 08, 2025

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 6 (CU6) corrige mais de 25 problemas relatados desde o lançamento do 2203 LTSR CU5.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

O que há de novo nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU5

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Aplicativos Virtuais e Desktops 7 2203 LTSR CU6

Novas implantações

Como faço para implantar o CU6 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU6 — usando o metainstalador do CU6. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Consulte a seção Citrix Virtual Apps and Desktops 7 2203 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 CU6 fornece atualizações para 15 (/pt-br/citrix-virtual-apps-desktops/2203-ltsr/whats-new/cumulative-update-4.html#2203-ltsr-5-baseline-components) do 2203 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU6. 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 2203 LTSR CU6

COMPONENTE DE LINHA DE BASE DO 2203 CU6	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.6000.6286	VDA de sessão única
VDA multissessão	2203.0.6000.6286	VDA multissessão
Delivery Controller	2203.0.6000.6286	Delivery Controller
Citrix Studio	7.33.6000.29	Citrix Studio
Citrix Director	7.33.6000.20	Citrix Director
Gerenciamento de Política de Grupo Citrix	7.33.6000.9	Gerenciamento de Política de Grupo Citrix
Extensão do Lado do Cliente da Política de Grupo Citrix	7.33.6000.9	
Citrix StoreFront	2203.0.6000.11	Citrix StoreFront
Citrix Provisioning	7.33.40	Citrix Provisioning
Servidor de Impressão Universal	7.33.6000.23	Universal Print Server
Gravação de Sessão	22.3.6000	Session Recording
Linux VDA	22.03.6000	Linux Virtual Delivery Agent
Gerenciamento de Perfis	22.3.6000.7	Profile Management
Citrix Federated Authentication Service	10.9.6000.9	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.32.6000.9	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2305	2305.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU6

Os componentes a seguir - 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 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2309	Citrix App Layering
HDX RealTime Optimization Pack	2.9.600	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	22.3.6000.11	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32.3000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	22.12.0	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Apenas a Atualização Cumulativa Mais Recente	Documentação

2203 LTSR CU6 exclusões notáveis

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. Especificamente, atualizações cumulativas e benefícios de ciclo de vida estendido são excluídos. Atualizações para recursos e componentes excluídos estão disponíveis através de versões atuais regulares.

COMPONENTES E RECURSOS EXCLUÍDOS
AppDisks™
AppDNA®
Pacote de Gerenciamento Citrix SCOM
Framehawk
vDisk Pessoal
Integração Online do Citrix StoreFront
Serviço de Ativação de Licença

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 2203 LTSR Cumulative Update 6 (CU6):

Suporte para colocar o disco WBC no mesmo local de armazenamento que o disco do SO

A partir da versão 2203 LTSR CU6, em ambientes de virtualização XenServer®, VMware e SCVMM, o MCS agora coloca o disco de cache de write-back (WBC) no mesmo local de armazenamento que o disco do SO se você configurar a lista de armazenamento do SO disponível da mesma forma que a lista de armazenamento temporário disponível ao criar uma conexão de host.

Esta implementação ajuda a reduzir a complexidade no gerenciamento dos discos do SO e WBC. Para criar uma conexão de host, consulte Conexões e recursos.

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU5:

Citrix Director

- Ao usar um VDA de desktop de sessão múltipla ou de sessão única em um Site de Múltiplas Florestas, o recurso de pesquisa centrado no usuário não funciona.
- No Director 2203, os usuários não conseguem editar e salvar políticas de Alerta Inteligente padrão devido a um destino de escopo inválido. A política funciona corretamente, mas falha na validação se o ID de destino for nulo ou inválido, resultando em uma mensagem de erro.
- Você pode encontrar um problema onde não consegue acessar Relatórios Personalizados
- Você pode não conseguir ver a lista de máquinas em Filtros do Director > Máquinas devido a valores Enum ausentes.

Política Citrix

- Você pode experimentar alta utilização de memória do processo CseEngine.exe, o que pode causar problemas de registro de máquina.

Citrix Studio

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

Delivery Controller™

- Você pode encontrar um problema onde a validação VUA falha durante as atualizações do VDA devido ao certificado renovado usando o nome da organização ou os nomes necessários.
- Você pode encontrar deadlocks frequentes no banco de dados SQL de Monitoramento e observar alto uso de CPU e memória para o serviço de monitoramento Citrix.
- Você pode encontrar um problema intermitente com o Machine Creation Services™ (MCS) no Citrix 2203 CU2, 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.

- 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%

Gráficos

- Você pode encontrar interrupções intermitentes na tela com duração de aproximadamente 10 segundos durante o trabalho, durante as quais o processo gráfico do software Citrix (Ctxgfx.exe) é redefinido. O thread twencode experimenta uma exceção de violação de acesso, o que faz com que o ctxExceptionHandler registre minidumps e cause esse problema. O ctxExceptionHandler está configurado para gerar dumps completos para exame.
- No Director local para CVAD 2203 LTSR CU2, você pode ver que as métricas de Brokering e "VM Start" sempre são exibidas como N/A. Isso ocorre quando os VDAs são configurados para iniciar somente quando você inicia um lançamento. Você pode encontrar esse problema ao revisar os dados de desempenho de logon.
- Você pode encontrar interrupções intermitentes na tela com duração de aproximadamente 10 segundos durante o trabalho, durante as quais o processo gráfico do software Citrix (Ctxgfx.exe) é redefinido. O thread twencode experimenta uma exceção de violação de acesso, o que faz com que o ctxExceptionHandler registre minidumps e cause esse problema. O ctxExceptionHandler está configurado para gerar dumps completos para exame.

Metainstalador

- Você pode experimentar um problema em que estados de Instância Gerenciada (MI) ausentes exigem reinicializações ou retomadas. Isso pode afetar a funcionalidade do VUA.
- Após a atualização do CVAD 2203 CU5, o arquivo `Microsoft.IdentityModel.Abstractions.dll` está ausente do diretório de instalação do Citrix Virtual Desktop Agent.

Servidor de Impressão Universal

Impressão

- Você pode experimentar um problema em que as impressoras não funcionam em sessões Citrix, resultando em vários erros de ID de Evento 1102 e 1106 devido a uma falha do Spooler de Impressão.
- O Serviço de Gerenciamento de Impressão Citrix pode ser encerrado intermitentemente, fazendo com que as impressoras redirecionadas parem de funcionar.

VDA para SO de sessão única

- Após a atualização para o CVAD 2203, você pode experimentar um atraso de aproximadamente 10 segundos ao abrir um desktop.
- Você pode encontrar um problema em que o serviço de Redirecionamento de Áudio Citrix falha no VDA do Citrix Cloud™, afetando a funcionalidade de áudio durante as sessões.

Área de Transferência

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

Sessão/Conexão

- 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.
- As impressoras mapeadas pelo cliente podem desaparecer após a reconexão se o serviço de spooler for reiniciado durante a sessão inicial. As impressoras permanecem visíveis ao reconectar do mesmo cliente.

Smart Cards

- 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%.

Exceções do Sistema

- Você pode experimentar uma falha do processo "explorer.exe" no Virtual Delivery Agent (VDA) ao usar o atalho "Windows + Print Screen".
- Você pode notar distorção de imagem ao gravar streams de webcams redirecionadas em aplicativos baseados em WebRTC durante uma sessão Citrix.
- Você pode experimentar desligamentos aleatórios de máquinas de sessão única ao fazer a transição para ou sair de períodos de interrupção quando não há sessão ativa.
- O suporte a FIDO2 não está disponível para aplicativos web de 32 bits nesta versão.

VDA para SO multissessão

- Ao reconectar a um Virtual Delivery Agent (VDA) provisionado com Machine Creation Services (MCS), ele pode se desregistrar devido a desconexões por inatividade, fazendo com que o VDA apareça como não registrado no Director. Esse problema também afeta VDAs não-MCS e ocorre quando os VDAs são desconectados via RDP ou deixados ociosos em uma sessão RDP.
- Você pode encontrar um problema em que o serviço de Redirecionamento de Áudio Citrix falha no Citrix Cloud VDA, impactando a funcionalidade de áudio durante as sessões.
- 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 publicado do Novo Microsoft Teams 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; ele funciona bem quando você está em uma sessão de desktop completa.

Área de Transferência

- Ao usar o VDA 2203 LTSR Cu4, e ao copiar e colar conteúdo no formato WebP, `WfShell` para de funcionar.
- Você pode ter problemas com a falha do 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.

Sessão/Conexão

- Você pode notar que o evento "MetaFrame 9006" é registrado toda vez que você se reconecta quando o Reconexão Automática do Cliente (ACR) está desabilitado, criando muitas mensagens de erro indesejadas.
- Você pode ter um problema em que os VDAs aleatoriamente param de responder e entram em um estado não registrado, fazendo com que os usuários sejam desconectados de suas sessões ICA.
- 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, mesmo que 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 foi reiniciado durante a sessão inicial. As impressoras permanecem visíveis ao reconectar do mesmo cliente.

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%.

Exceções do Sistema

- Você pode encontrar problemas com o redirecionamento do Windows Media ao reproduzir um vídeo em uma configuração multi-sessão.
- Você pode ter falhas do TermService com o Citrix VDA.
- Você pode ter um problema em que o status da bateria não é exibido no VDA multi-sessão do Windows 11, apesar de o VDA estar recebendo o status da bateria.
- Um bugcheck 0x50 pode ocorrer em wdica32.exe ao ler o estado da licença.

Citrix Provisioning™

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

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.

Atualização Cumulativa 5 (CU5)

Data de lançamento: Jun 04, 2024

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 5 (CU5) corrige mais de 25 problemas relatados desde o lançamento do 2203 LTSR CU4.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

O que há de novo nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU4

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Aplicativos e Desktops Virtuais 7 2203 LTSR CU5

Novas implantações

Como faço para implantar o CU5 do zero?

Você pode configurar um ambiente Citrix Virtual Apps and Desktops totalmente novo baseado no CU5 - usando o metainstalador do CU5. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Consulte a seção Citrix Virtual Apps and Desktops 7 2203 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 CU5 fornece atualizações para 15 componentes de linha de base do 2203 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR da sua implantação para o CU5. 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 2203 LTSR CU5

COMPONENTE DE LINHA DE BASE DO 2203 CU5	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.5000.5310	VDA de sessão única
VDA multissessão	2203.0.5000.5310	VDA multissessão
Delivery Controller	2203.0.5000.5310	Delivery Controller
Citrix Studio	7.33.5000.17	Citrix Studio
Citrix Director	7.33.5000.16	Citrix Director
Gerenciamento de Política de Grupo do Citrix	7.33.5000.10	Gerenciamento de Política de Grupo do Citrix
Extensão do Lado do Cliente da Política de Grupo do Citrix	7.33.5000.9	
Citrix StoreFront	2203.0.5000.6	Citrix StoreFront
Citrix Provisioning	7.33.40	Citrix Provisioning
Servidor de Impressão Universal	7.33.5000.8	Universal Print Server
Gravação de Sessão	22.3.5000	Session Recording
Linux VDA	22.03.5000	Linux Virtual Delivery Agent
Gerenciamento de Perfis	22.3.5000.2	Profile Management

COMPONENTE DE LINHA DE BASE DO 2203 CU5	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
Citrix Federated Authentication Service	10.9.5000.8	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.32.5000.7	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2305	2305.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU5

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 somente de correção). A Citrix® pode solicitar que você atualize para uma versão mais recente desses componentes em seus ambientes 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2309	Citrix App Layering
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	24.3.2	Camada de personalização do usuário
Reprodutor web de gravação de sessão	22.3.5000.2	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32.3000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	22.12.0	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

2203 LTSR CU5 exclusões notáveis

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. 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
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 do ciclo de vida de fornecedores terceirizados.

O que há de novo

Não há novos recursos e aprimoramentos no Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 5 (CU5).

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU4:

Citrix Director

- Quando você usa um VDA de desktop de sessão múltipla ou de sessão única em um Site de Múltiplas Florestas, o recurso de pesquisa centrado no usuário não funciona.

Política Citrix

- Ao instalar o Studio em uma máquina Windows 11 Multi-Sessão e abrir o Console de Gerenciamento de Política de Grupo, a seguinte mensagem de erro é exibida ao carregar os módulos de Política de Grupo Citrix: `ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.`

- O Citrix Studio exibe incorretamente o grupo de entrega `uuid` em vez do nome em Atribuído a na guia **Políticas**.

Citrix Studio

Delivery Controller™

- Ao adicionar o endereço do servidor StoreFront™ através do Citrix Studio e atribuí-lo a um Grupo de Entrega, a loja é definida como desativada por padrão.

Delivery Controller™

- A tarefa de criar\atualizar catálogo de máquinas falha na Zona de Disponibilidade B, mas funciona bem para as Zonas de Disponibilidade A e C porque uma instância de serviço de volume não pôde ser iniciada em sua conexão de nuvem. Execute o comando abaixo para atualizar a tabela do Banco de Dados do Site para usar o novo VolumeWorkerTemplate no servidor SQL. `UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate SET TemplateId = 'ami-09b42976632b27e9b' WHERE RegionName = 'ap-southeast-2'`

> **Nota:**

> A Zona de Disponibilidade pode ser diferente para clientes diferentes.

- Após a reinicialização do hipervisor, as VMs não iniciam porque o gerenciamento de energia de pico está configurado.
- Os recursos publicados podem falhar ao enumerar quando o campo de senha está vazio.

Gráficos

- Ao usar o Citrix Virtual Apps and Desktops 2203, você pode observar uma tela preta ao se reconectar às sessões desconectadas.

Metainstalador

- 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.
- A tentativa de atualizar o Citrix Virtual Apps and Desktops da versão 1912 LTSR para a versão 2305 ou 2203 LTSR pode falhar com esta mensagem de erro: Descobrimos uma configuração não suportada.

Otimização do Microsoft Teams

- O Microsoft Teams 2.1 não é otimizado por padrão no VDA.

Monitor

- As atualizações na tabela `MonitorData.ResourceUtilization` no banco de dados de monitoramento estão atrasadas.

Servidor de Impressão Universal

Impressão

- O Citrix Universal™ Print Server pode não funcionar como esperado ao remover o grupo Todos das permissões de segurança da impressora.
- O driver HP Color LaserJet 2800 Series PS, instalado conforme descrito no artigo CTX140208 do Knowledge Center, pode ser desinstalado durante a atualização do VDA.
- 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 VDA Windows 10, as impressoras que usam CUPS exibem a seguinte mensagem:

`Access Denied, cannot connect message`

VDA para SO de sessão única

Teclado

- 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.
- A opção de copiar para a área de transferência no aplicativo remoto publicado não está funcionando para as versões CU3 e CU4.

Sessão/Conexão

- O processo `WebSocketService.exe` falha ao iniciar após a reinicialização de um VDA no dia bissexto.
- Ao usar um VDA do Windows 10 versão 2308, o processo `ctxappvservice.exe` pode falhar.
- Ao usar as versões Citrix VDA LTSR 1912 CU3 e posteriores, e o sistema tiver conexões anexadas e parecer mais provável com o número de usuários anexados, o Citrix HDX™ HTML5 Video pode falhar.
- Durante uma reconexão de sessão ICA, a janela de bate-papo de um aplicativo de mensagens de terceiros pode aparecer automaticamente em primeiro plano.
- Ao usar uma máquina, o lançamento da sessão do usuário falha intermitentemente.
- Ao conectar-se a um Windows 10 com VDA 2203 CU3 instalado a partir de um endpoint do Windows 10 com Citrix Workspace™ App versão 2210 ou 2303, a sessão é desconectada ao tentar selecionar uma câmera em um aplicativo WebRTC.
- Os VDAs podem se desregistrar intermitentemente quando o IPv6 está ativado.
- A tentativa de reconectar a uma sessão VDA no Citrix Virtual Apps and Desktops versão 2203 LTSR CU2 usando um cartão inteligente pode resultar em uma tela de Boas-vindas travada.
- Ao iniciar um desktop virtual (win10 multi-sessão) e conectar um fone de ouvido, há um atraso significativo no som do UAC enquanto você ajusta o volume do áudio do sistema.
- A cópia de conteúdo de um aplicativo Microsoft Visio ou Visio publicado em um desktop para um aplicativo no dispositivo do usuário pode falhar.
- A mensagem que aparece na caixa de diálogo de aviso do Citrix HDX 3D Pro em um sistema operacional não inglês pode aparecer corrompida.

- Ao iniciar uma sessão que se conecta a um VDA que está executando a versão 2203 LTSR CU2 e tem o Microsoft Defender Application Control instalado, uma tela cinza pode aparecer por alguns segundos.
- No acesso remoto a PC, alguns eventos são registrados em "Citrix-HostCore-ICA Service/Admin". Quando a sessão foi desconectada usando **Ctrl+Alt+Del**, os IDs de evento 43 e 46 foram registrados. No VDA do SO em inglês, funcionou como esperado. No VDA do SO em japonês, os IDs de evento de 37 a 50 não foram registrados no "Citrix-HostCore-ICA Service".
- O serviço de navegador verifica se `ctxcsb` está disponível no endpoint; se não estiver disponível, honra a troca de capacidade BCR através de GVCH e desativa o recurso.
- Se você fizer login com a Conta Microsoft no Excel ou Word e o redirecionamento de pasta especial estiver ativado, o Excel ou Word 365 trava em `sfrhook.dll` após abrir e digitar alguns caracteres. O problema não ocorre se o redirecionamento de pasta especial estiver desativado.
- O processo do Terminal Services pode travar após uma reconexão ACR.
- Ao configurar o redirecionamento de conteúdo do navegador com o modo SFCR, a página da web BCR pode não conseguir carregar a página completa.
- O aplicativo **OpenTEXT ETX** não abre devido a violação de acesso com o seguinte módulo:

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

- 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, Citrix Workspace app 2203 LTSR CU3 (2303 ou 2205) e VDA 2203 LTSR com Windows 11 22h2.
- Se as impressoras ou servidores de impressão estiverem inacessíveis, o logon e o logoff da sessão podem demorar muito para responder.

Exceções do Sistema

- Ao usar um VDA, você pode experimentar uma exceção fatal em picadd.sys e exibir uma tela azul com um código de verificação de erro 0x96. Isso se aplica a todos os sistemas operacionais.
- Ao usar um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de erro com a mensagem `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys` a qualquer momento no início ou durante uma sessão.

VDA para SO multissessão

Teclado/Mouse

- No Windows Server 2022, se um mouse for movido para uma posição dedicada pelo aplicativo ou SO, você não poderá mover o mouse para essa posição novamente até que o mouse seja movido para outro local pelo aplicativo ou SO.
- A opção de copiar para a área de transferência no aplicativo remoto publicado não está funcionando para as versões CU3 e CU4.

Sessão/Conexão

- O processo `WebSocketService.exe` falha ao iniciar após uma reinicialização do VDA no dia bissexto.
- A caixa de diálogo Mensagem de Aviso de Tempo Ocioso Expirado não aparece na sessão ICA no VDA do SO 2022, embora o limite de tempo ocioso da sessão entre em vigor.
- Na versão LTSR 2203 CU3 do VDA do Server 2019, `WmiPrvSE.exe` falha.
- Ao usar as versões Citrix VDA LTSR 1912 CU3 e posteriores, e o sistema possui conexões anexadas, sendo mais provável que ocorra com um maior número de usuários conectados, o Citrix HDX HTML5 Video pode falhar.
- Alguns processos do aplicativo Citrix Workspace podem não fechar conforme o esperado quando executados em uma sessão de aplicativo publicado.
- O processo do Terminal Services pode falhar após uma reconexão ACR.
- Quando você define o redirecionamento de conteúdo do navegador com o modo SFCR, a página da web do BCR pode não conseguir carregar a página completa.
- O aplicativo **OpenTEXT ETX** falha ao abrir devido a violação de acesso com o seguinte módulo:

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

- Se as impressoras ou servidores de impressão estiverem inacessíveis, o logon e o logoff da sessão podem levar muito tempo para responder.
- O WebSocketService (Serviço WebSocker de Redirecionamento de Vídeo HTML5) pode falhar.

Exceções do Sistema

- Ao usar um VDA, você pode encontrar uma exceção fatal em picadd.sys e exibir uma tela azul com um código de verificação de erro 0x96. Isso se aplica a todos os sistemas operacionais.

- Ao usar um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de erro com a mensagem `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys` a qualquer momento no início ou durante uma sessão.

Citrix Provisioning™

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

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.

Atualização Cumulativa 4 (CU4)

Data de lançamento: November 16, 2023

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Atualização Cumulativa 4 (CU4) corrige mais de 60 problemas relatados desde o lançamento do 2203 LTSR CU3.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

Novidades nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU3

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Virtual Apps e Desktops 7 2203 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 2203 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 2203 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 2203 LTSR CU4

COMPONENTE DE LINHA DE BASE DO 2203 CU4	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.4000.4310	VDA de sessão única
VDA de múltiplas sessões	2203.0.4000.4310	VDA de múltiplas sessões

COMPONENTE DE LINHA DE BASE DO 2203 CU4	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
Delivery Controller	2203.0.4000.4310	Controlador de Entrega
Citrix Studio	7.33.4000.15	Citrix Studio
Citrix Director	7.33.4000.26	Citrix Director
Citrix Group Policy Management	7.33.4000.2	Citrix Group Policy Management
Citrix Group Policy Client-Side Extension	7.33.4000.5	
Citrix StoreFront	2203.0.4000.13	Citrix StoreFront
Citrix Provisioning	7.33.40	Provisionamento Citrix
Servidor de Impressão Universal	7.33.4000.11	Servidor de Impressão Universal
Gravação de Sessão	22.3.4000	Gravação de Sessão
Linux VDA	22.03.3000.6	Agente de Entrega Virtual Linux
Gerenciamento de Perfis	22.3.4000.7	Gerenciamento de Perfil
Serviço de Autenticação Federada Citrix	10.9.4000.6	Serviço de Autenticação Federada Citrix (FAS)
Redirecionamento de Conteúdo do Navegador	15.32.4000.12	Redirecionamento de Conteúdo do Navegador
Agente de Sondagem Citrix 2305	2305.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU4

Os componentes a seguir - 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 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2309	Citrix App Layering
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Servidor de Licenças	11.17.2.0_BUILD_44000	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 do Ambiente de Trabalho	22.12.0	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa Mais Recente	Documentação

2203 LTSR CU4 exclusões notáveis

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. 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 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

Não há novos recursos e aprimoramentos no Citrix Virtual Apps and Desktops 7 2203 LTSR Cumulative Update 4 (CU4).

Problemas corrigidos

Problemas corrigidos na Atualização Cumulativa 4 (CU4) do 2203 LTSR, Atualização 1

VDA para SO de sessão única e multi-sessão

EXCEÇÃO DO SISTEMA

- Os VDAs podem apresentar uma exceção fatal em picadd.sys e exibir uma tela azul com a seguinte mensagem de erro:

  Erro: Verificação de Bug 0x96 INVALID_WORK_QUEUE_IT

> **Observação:**
>
> Esta correção está disponível apenas nos instaladores mínimos da Atualização 1 do CU4.

Problemas corrigidos na Atualização Cumulativa 4 (CU4) do 2203 LTSR

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU3:

Citrix Director

- O uso da memória pode não ser exibido em **Citrix Director console > Trends > Load Evaluator Index**.
- No Citrix Director, o uso da máquina em **Director console > Trends > Machine Usage > Multi-session OS Machines** aparece como 0 (Zero) na coluna Em Uso para todos os Delivery Groups.

Citrix Policy

- O valor da política de canal virtual **VirtualChannelWhiteList** na configuração HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\VCPolicies pode ser corrompido e falhar ao ser aplicado no VDA após a reinicialização. Esse problema ocorre quando você exclui arquivos da pasta C:\ProgramData\Citrix\GroupPolicy ou recorta o conteúdo da pasta e o cola em um local diferente.
- O valor de Modelagem de Política de Grupo mostra o valor desabilitado em vez do valor real. Por exemplo, o valor **Unidade de memória de exibição** é exibido como desabilitado em vez do valor real, 65536 KB.
- Tentativas de aplicar políticas de usuário Citrix em domínios diferentes podem falhar ao atualizar um VDA para a versão LTSR CU7.
- Ao selecionar um usuário no **Citrix Group Policy Modelling Wizard** e escolher a opção **Skip to the final page of the wizard without collecting additional data**, esta mensagem de erro pode aparecer na página **Summary**:

  O valor não pode ser nulo.

  Chave do nome do parâmetro

- Após uma redefinição de perfil, o redirecionamento de pasta pode falhar intermitentemente.

Citrix Studio

- A visualização de Log no Citrix Studio pode não exibir dados.

Delivery Controller™

- Certos contadores de desempenho XML do Citrix podem não ser adicionados ao gráfico do monitor de desempenho.
- Tentativas de criar uma nova conexão de hospedagem no mestre do pool XenServer® podem falhar com esta mensagem de erro:

  Não é possível contatar o servidor host. Verifique se a conexão tem um endereço de host válido e se o servidor host está ligado e funcionando corretamente.

  Falha ao obter a lista de hosts XenServer.

- Os VDAs podem falhar ao registrar e podem permanecer presos no estado de inicialização com a contagem de sessões mostrando -1.
- Quando um VDA persistente executando o Microsoft Windows 11 redefine a senha, você pode não conseguir fazer logon no VDA. Uma mensagem de erro de falha de relacionamento de confiança de domínio pode aparecer no log de eventos uma vez a cada 30 dias.
- Ao criar catálogos de máquinas AWS, o volume prepare-identity pode não ser removido automaticamente mesmo após a máquina virtual de preparação correspondente ter sido encerrada e excluída.
- Com esta correção, o Machine Creation Services™ oferece suporte ao vSAN 8.

Metainstalador

- Ao instalar o VDA para SO multi-sessão com a opção **Habilitar conexões para uma máquina de servidor** habilitada e atualizar o VDA, o texto **Componentes Adicionais para Imagem MCS Mestra** é exibido no assistente de atualização em vez de **Componentes Adicionais para Habilitar Conexões Intermediadas a um Servidor**.

> **Observação:**
>
> Esta correção é aplicável a partir do Citrix Virtual Apps and Desktops 1912 LTSR CU8 e atualizações de CUs 1912 LTSR para 1912 LTSR CU8 e superior. No entanto, a correção não é aplicável para XenApp and XenDesktop 7.15 LTSR CUs e atualizações de XenApp and XenDesktop 7.15 LTSR para Citrix Virtual Apps and Desktops 1912 LTSR CUs.

Servidor de Impressão Universal

CLIENTE

- O serviço Spooler de Impressão pode ser encerrado inesperadamente ao imprimir um arquivo usando o Citrix Universal™ Print Server.

VDA para SO de sessão única

INSTALANDO, DESINSTALANDO, ATUALIZANDO

- Quando você atualiza o Citrix Virtual Apps and Desktops 2203 LTSR do CU1 para o CU2, os valores **EnableVistaMousePointers**, **EnforceUserPolicyEvaluationSuccess**, **Flag** e **CitrixDoD** que foram criados manualmente nas seguintes chaves de registro podem desaparecer:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

    Nome: `EnableVistaMousePointers`

    Tipo: DWORD

    Valor: 1
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`

    Nome: `EnforceUserPolicyEvaluationSuccess`

    Tipo: DWORD

    Dados: 0
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Smart Card Hook`

    Nome: `Flag`

    Tipo: DWORD

    Valor: 0
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits

    Nome: `CitrixDoD`

    Tipo: DWORD

    Valor: 0

- Depois de atualizar um VDA para 1912 LTSR CUx ou 2203 LTSR CUx, o valor de **ApplicationLaunchWaitTimeoutMS** na chave de registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI pode não ser restaurado.

TECLADO

- Ao alternar entre layouts de teclado como Reino Unido e Estados Unidos, podem ocorrer problemas intermitentes de idioma com o teclado na sessão.
- Ao usar o aplicativo Citrix Workspace™ no Ubuntu com a versão VDA 2203 LTSR CU3 ou anterior, a sincronização do layout do teclado pode não funcionar corretamente. Por exemplo, se um usuário alterar os layouts de teclado local e do lado do servidor de inglês para alemão, o teclado pode exibir uma saída de caractere incorreta, mesmo que ambos os teclados tenham layouts alemães.

IMPRESSÃO

- Quando você reinicia um VDA com as políticas do Universal Print Server ativadas, o balanceamento de carga para Universal Print Servers pode falhar ao iniciar.
- As impressoras locais podem não ser redirecionadas para a sessão durante o primeiro lançamento. No entanto, as impressoras locais são redirecionadas durante os lançamentos subsequentes.

SESSÃO/CONEXÃO

- O serviço de Áudio do Windows pode não iniciar automaticamente ao instalar o Virtual Delivery Agent usando o parâmetro de linha de comando `servervdi`. Esta mensagem de erro aparece na área de notificação:

  O Serviço de Áudio não está em execução.

- As sessões podem permanecer presas no estado de **Desconexão** no Cloud Studio ou Monitor até que o sistema seja inicializado. O problema ocorre quando os VDAs do RemotePC são desligados de dentro do RemotePC.
- Quando você copia conteúdo da sessão 1 usando o mapeamento da área de transferência e tenta colá-lo na sessão 2, o conteúdo pode não aparecer na área de transferência da sessão 2. O problema ocorre quando a sessão 2 é iniciada depois que o conteúdo é copiado da sessão 1.
- Depois de atualizar um VDA para a versão 2203, o aplicativo Skype for Business pode exibir uma tela inicial ao ser iniciado e ficar sem resposta.

- O mapeamento de unidade cliente (CDM) pode não funcionar em um VDA recém-instalado versão 2203 LTSR CU2 executando o Microsoft Windows Server quando o Serviço Citrix Print Manager está desativado.
- Quando o recurso Shellbridge está habilitado no VDA, as sessões de aplicativos contínuas do HTML5 e Android podem mostrar janelas de interface do usuário inesperadas que podem bloquear a entrada do usuário.
- Os valores **SaveRsopToFile**, **SaveRsopToMemory** e **SaveRsopToRegistry** sob a chave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy podem não ser restaurados.
- O Redirecionamento de Áudio Citrix pode falhar ao funcionar com o VDA versão 2203 LTSR CU3 quando mais de oito dispositivos de áudio estão conectados a um dispositivo de usuário.
- O redirecionamento da Webcam pode falhar no aplicativo Citrix Workspace para Mac executando o macOS Ventura.
- A tentativa de iniciar aplicativos com um arquivo ICA® personalizado pode falhar após a atualização do VDA para a versão 2203 LTSR CU3.
- Se o agente de Gravação de Sessão não estiver instalado no VDA e você executar os comandos PowerShell **Get-BrokerSessionRecordingStatus**, **Start-BrokerSessionRecording** e **Stop-BrokerSessionRecording**, o VDA se desregistra e se registra novamente com o Delivery Controller em poucos segundos. Esta ação não tem impacto nas sessões existentes. Se o agente de Gravação de Sessão estiver instalado no VDA, os comandos PowerShell funcionam sem problemas.

CARTÕES INTELIGENTES

- Ao iniciar uma sessão usando um cartão inteligente e tentar desbloquear uma sessão bloqueada, você pode receber um prompt para inserir uma senha em vez de um PIN de cartão inteligente. Esse problema ocorre quando você instalou o patch da Microsoft, KB5018410.
- CtxSvcHost (CtxSmartCardSvc) pode ser encerrado inesperadamente ao fazer logoff do VDA.

EXCEÇÕES DO SISTEMA

- Sites internos de certas aplicações de terceiros com VDA instalado podem não permitir acesso sem um prompt.
- O driver da Impressora Universal Citrix PDF pode ser encerrado inesperadamente devido ao módulo acfpdfuamd64.dll com falha.
- O processo wfica32.exe pode ser encerrado inesperadamente.
- Os VDAs podem apresentar uma exceção fatal em Wdica.sys e exibir uma tela azul.

- O processo de gráficos de software Citrix (Ctxgfx.exe) pode consumir constantemente toda a memória disponível em uma sessão, fazendo com que ela eventualmente se desconecte.
- O processo do indicador de status gráfico, GfxStatusIndicator.exe, pode ser encerrado repetidamente.
- Depois de atualizar um VDA da versão 2203 LTSR CU2 para CU3, os VDAs podem apresentar uma exceção fatal em picadm.sys e exibir uma tela azul.

EXPERIÊNCIA DO USUÁRIO

- O processo wfshell.exe pode parar de responder ao copiar e colar grandes volumes de dados no Microsoft Excel.

VDA para SO multi-sessão

TECLADO

- Após atualizar um VDA para a versão 2305 ou 2203 LTSR CU3, as combinações de teclas de atalho podem não funcionar corretamente. Por exemplo, em um documento do Word, pressionar a tecla **Ctrl+Shift+K** em uma palavra selecionada a colocava em maiúsculas. Mas, se você soltar a tecla **K** e pressioná-la novamente, a alteração não é revertida.
- Ao usar o aplicativo Citrix Workspace no Ubuntu com VDA versão 2203 LTSR CU3 ou anterior, a sincronização do layout do teclado pode não funcionar corretamente. Por exemplo, se um usuário alterar os layouts de teclado local e do lado do servidor de inglês para alemão, o teclado poderá exibir uma saída de caractere incorreta, mesmo que ambos os teclados tenham layouts alemães.

IMPRESSÃO

- Ao reiniciar um VDA com as políticas do Universal Print Server ativadas, o balanceamento de carga para os Universal Print Servers pode falhar ao iniciar.
- As impressoras locais podem não ser redirecionadas para a sessão durante o primeiro lançamento. No entanto, as impressoras locais são redirecionadas durante os lançamentos subsequentes.

SESSÃO/CONEXÃO

- As sessões podem permanecer presas no estado de Logging Off no Cloud Studio ou Monitor até que o sistema seja inicializado. O problema ocorre quando os VDAs do RemotePC são desligados de dentro do RemotePC.
- As tentativas de abrir arquivos PDF usando o Adobe Acrobat Reader DC em servidores Citrix podem falhar com esta mensagem de erro:

Werfault.exe - Erro de Aplicativo

O aplicativo não pôde ser iniciado corretamente (0xc0000142). Clique em Ok para fechar o aplicativo.

- A Gravação de Sessão pode continuar a gravar mesmo depois que você faz logoff da sessão ou se a sessão for desconectada.
- Ao alternar entre endpoints sem desconectar a sessão, várias notificações de reinicialização podem aparecer se as notificações de reinicialização agendadas estiverem ativadas.
- Ao abrir 2 instâncias de um aplicativo e definir a configuração **DisableToggler** para cinco segundos, você pode ter que esperar cerca de 30 segundos antes de digitar no segundo aplicativo.
- Ao copiar conteúdo da sessão 1 usando o mapeamento da área de transferência e tentar colá-lo na sessão 2, o conteúdo pode não aparecer na área de transferência da sessão 2. O problema ocorre quando a sessão 2 é iniciada após o conteúdo ser copiado da sessão 1.
- Depois de atualizar um VDA para a versão 2203, o aplicativo Skype for Business pode exibir uma tela inicial ao ser iniciado e ficar sem resposta.
- Ao reconectar a uma sessão após alterar o valor de DPI do cliente, o novo valor pode não ser aplicado à sessão.
- Depois de atualizar o VDA para a versão 2203 LTSR CU2, os VDAs podem se desregistrar.
- A tentativa de iniciar aplicativos com um arquivo ICA personalizado pode falhar após a atualização do VDA para a versão 2203 LTSR CU3.
- O redirecionamento da webcam pode falhar no aplicativo Citrix Workspace para Mac executando o macOS Ventura.
- Se o shellbridge estiver ativado, talvez você não consiga fazer logoff de uma sessão clicando no ícone **X** na janela.
- Com esta correção, as notificações pop-up podem aparecer corretamente em sessões contínuas. Você deve habilitar o shellbridge para que a correção funcione. No entanto, a correção é implementada com as seguintes limitações visuais:
  - Um fundo preto. envolve a notificação pop-up.
  - A notificação pop-up cobre algumas das áreas da barra de tarefas local.

CARTÕES INTELIGENTES

- Ao iniciar uma sessão usando um cartão inteligente e tentar desbloquear uma sessão bloqueada, você pode receber um prompt para inserir uma senha em vez de um PIN do cartão inteligente. Esse problema ocorre quando você instalou o patch da Microsoft, KB5018410.
- O CtxSvcHost (CtxSmartCardSvc) pode ser encerrado inesperadamente ao fazer logoff do VDA.

EXCEÇÕES DO SISTEMA

- O driver da Impressora Universal PDF da Citrix pode ser encerrado inesperadamente devido ao módulo acfpdfuamd64.dll com falha.
- O processo wfica32.exe pode ser encerrado inesperadamente.
- Os VDAs podem apresentar uma exceção fatal em Wdica.sys e exibir uma tela azul.
- O Serviço de Redirecionamento de Vídeo Citrix HDX HTML5 (WebSocketService.exe) pode ser encerrado inesperadamente ao usar o Microsoft Teams.
- Depois de atualizar um VDA da versão 2203 LTSR CU2 para CU3, os VDAs podem apresentar uma exceção fatal em picadm.sys e exibir uma tela azul.

EXPERIÊNCIA DO USUÁRIO

- O processo wfshell.exe pode parar de responder ao copiar e colar grandes volumes de dados no Microsoft Excel.

INTERFACE DO USUÁRIO

- No Windows Server versão 2019 e anteriores, os VDAs podem falhar ao enviar eventos do mouse para o endpoint, causando problemas gráficos ou do mouse nos aplicativos.

Citrix Provisioning™

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.

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 3 (CU3)

Data de lançamento: June 1, 2023

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Atualização Cumulativa 3 (CU3) corrige mais de 60 problemas relatados desde o lançamento do 2203 LTSR CU2.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

Novidades nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU2

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Aplicativos Virtuais e Desktops 7 2203 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:

Examine a seção Citrix Virtual Apps and Desktops 7 2203 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 CU3 fornece atualizações para 15 componentes de linha de base do 2203 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 2203 LTSR CU3

COMPONENTE DE LINHA DE BASE DO 2203 CU3	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.3000.3300	VDA de sessão única
VDA de múltiplas sessões	2203.0.3000.3300	VDA de múltiplas sessões
Delivery Controller	2203.0.3000.3300	Delivery Controller
Citrix Studio	7.33.3000.18	Citrix Studio
Citrix Director	7.33.3000.24	Citrix Director
Citrix Group Policy Management	7.33.3000.10	Citrix Group Policy Management
Citrix Group Policy Client-Side Extension	7.33.3000.17	
Citrix StoreFront	2203.0.3000.14	Citrix StoreFront
Citrix Provisioning	2203.0.17	Citrix Provisioning
Servidor de Impressão Universal	2203.0.3000.9	Universal Print Server

COMPONENTE DE LINHA DE BASE DO 2203 CU3	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
Gravação de Sessão	22.3.3000	Session Recording
Linux VDA	22.03.3000.6	Linux Virtual Delivery Agent
Gerenciamento de Perfis	22.3.3000.3	Profile Management
Citrix Federated Authentication Service	10.9.3000.10	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.32.3000.7	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2305	2305.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU3

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 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	23.4.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Servidor de Licenças	11.17.2.0 compilação 42000	Servidor de Licenças
Camada de personalização do usuário	23.4.0	Camada de personalização do usuário
Reprodutor web de Gravação de Sessão	22.3.3000.4	Reprodutor web de gravação de sessão

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
Otimização do Microsoft Teams	15.32.3000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	22.12.0	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa Mais Recente	Documentação

Exclusões notáveis do 2203 LTSR CU3

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. 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
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.

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU2:

Citrix Director

- Depois que uma sessão é estabelecida, o nome de exibição da máquina na página Detalhes da Máquina no Citrix Director reverte para o nome do Grupo de Entrega.

Citrix Policy

- Com esta correção, vários problemas de memória foram corrigidos.
- O valor da configuração da política pode aparecer como **Kpbs** em vez de **Kbps**.

Delivery Controller™

- Se a agregação de Site ou grupos de entrega com políticas de broker específicas estiverem habilitados, iniciar um aplicativo ou uma área de trabalho cria uma nova sessão em vez de reconectar-se a uma existente.
- As tentativas de criar um catálogo de máquinas MCS podem falhar quando a porta HTTPS 443 está em uso.
- Quando a memória reservada é menor que a memória configurada, as tentativas de ligar uma máquina virtual podem falhar com esta mensagem de erro:

  Configuração de memória inválida: A reserva de memória (sched.mem.min) deve ser igual a memsize (94208). A máquina virtual falhou ao iniciar. Falha ao ativar o módulo MemSched. Erro ao analisar os parâmetros de configuração específicos do agendador.

- O Citrix Broker Service (Brokerservice.exe) pode ser encerrado inesperadamente após a desconexão do Servidor de Licenças.
- Esta correção melhora o desempenho geral do Citrix Virtual Apps and Desktops 2203 LTSR.
- Com esta correção, NT5DS é o protocolo de sincronização de tempo padrão em cenários onde:

  a. A imagem mestre não está associada ao domínio (NDJ) e
  b. Durante o provisionamento do MCS, você seleciona a VM para ser Active Directory (AD) ou Hybrid Azure Active Directory (HAAD)

- Com esta correção, 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 `parameter -NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede. Para obter mais informações, consulte Alterar a configuração de rede para um esquema de provisionamento existente.

Serviço de Autenticação Federada

- Você não consegue instalar o VDA em um desktop Windows 11. Você recebe o seguinte erro:

  A instalação do plug-in VDA de asserção de identidade de autenticação Citrix falhou com o código de erro 1603.

Licenciamento

- O Citrix Studio (snap-in do PowerShell do Administrador de Licenciamento) pode falhar ao se comunicar com os servidores de Licenciamento somente quando conjuntos de cifras fortes são permitidos.

Otimização do Microsoft Teams

- O Serviço de Redirecionamento de Vídeo HTML5 (CtxHdxWebSocketService) pode ser encerrado inesperadamente.

Metainstalador

- O instalador do Delivery Controller está faltando a opção de linha de comando ***/ No_Pending_Reboot_Check*** na versão 2203 LTSR, que estava disponível nas versões 1912.
- Ao atualizar um VDA, a configuração da chave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode pode ser excluída.
- Tentativas de atualizar um VDA para a versão 2203 LTSR CU2 podem falhar.

Problemas de Segurança

- Esta correção aborda um problema de segurança. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX559370.

Servidor de Impressão Universal

Servidor

- O serviço Citrix XTE pode ser encerrado inesperadamente no Universal Print Server, fazendo com que os trabalhos de impressão permaneçam presos na fila.
- O processo EMFPrint.exe pode ser encerrado inesperadamente no Citrix Universal Print Server 2203.

VDA para SO de sessão única

Instalando, Desinstalando, Atualizando

- Tentativas de atualizar um VDA da versão 1912 LTSR CU3 para a versão 2203 LTSR CU2 podem falhar.
- 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.
- Com esta correção, a ferramenta VUA compara a versão principal ao realizar atualizações, permitindo atualizações de lançamento de CU. Agora você pode realizar atualizações LTSR como 2203.0.0.x para 2203.0.1000.x (CU1).
- Com o recurso 'Habilitar restauração em caso de falha' ativado, os pontos de restauração podem não ser criados durante a atualização ou instalação dos VDAs.

Teclado

- O teclado virtual pode não aparecer automaticamente em um aplicativo publicado quando você posiciona o cursor em um campo editável.

Sessão/Conexão

- As tentativas de imprimir um documento do Citrix Universal™ Print Server nas impressoras de sessão compartilhada podem falhar. O problema ocorre após a atualização para o Citrix Virtual Apps and Desktops 1912 LTSR CU4.
- A chave de redirecionamento do Microsoft Teams **MSTeamsRedirSupport** no registro HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream pode estar ausente ao reconectar a um dispositivo de usuário por meio de uma sessão de usuário. O problema ocorre quando uma sessão RDP ainda existe.
- As tentativas de reconectar-se a uma sessão podem falhar.

- Quando você assume sua sessão de usuário atualmente conectada a partir de um console local de um VDA físico, todos ou alguns monitores conectados ao VDA físico podem permanecer no modo de economia de energia.
- Tentativas de instalar um VDA versão 2203 podem falhar quando o sistema Windows não tem uma unidade C.
- Depois de atualizar um VDA para a versão 2203, o aplicativo Skype for Business pode parar de responder na tela inicial.
- Ao conectar um monitor, a janela contínua pode desaparecer.
- Em um cenário de salto duplo, você pode ver duas webcams extras não utilizadas durante o primeiro salto.
- Em um VDA versão 2203 executando no Microsoft Windows 10 versão 21H2, o menu Iniciar do Windows pode exibir uma caixa vazia em vez da opção **Energia > Desconectar**.
- O serviço ICA® pode não abrir em VDAs Windows 10 H2 não ingressados no domínio e não em inglês.
- Com esta correção, o redirecionamento de conteúdo bidirecional suporta o uso de curingas ao definir as URLs a serem redirecionadas. Para obter mais informações, consulte Redirecionamento de curinga do Citrix VDA para o cliente.
- Tentativas de compartilhar certos aplicativos personalizados usando o Microsoft Teams otimizado podem falhar.
- Com o shellbridge ativado, todos os programas de inicialização são iniciados em uma sessão de aplicativo publicado HDX™. Sair de um aplicativo pode impedir um logoff gracioso. Se o problema persistir, defina o valor como 0 no seguinte registro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  Nome: Shellbridge

  Tipo: REG_DWORD

  Valor: 0

- As máquinas em pool que estão **LIGADAS** podem ser desligadas automaticamente e se tornarem não registradas. [
- Quando dispositivos de áudio são adicionados a uma sessão de usuário, você não consegue ouvir sons de nenhum dos dispositivos, exceto os sons do Skype for Business. Esta mensagem de erro aparece:

Erro - não há mais slots de dispositivo disponíveis - falha ao adicionar o dispositivo.

O problema ocorre quando mais de oito dispositivos de reprodução ou gravação são conectados a um endpoint.

Exceções do Sistema

- O serviço CseEngine.exe pode consumir mais memória do que o esperado nos VDAs.
- O Serviço Citrix HDX RAVE (CtxSvcHost.exe) pode ser encerrado inesperadamente.
- Ao iniciar um desktop publicado, abrir o **Explorador de Arquivos** e clicar na unidade C local redirecionada em **Rede > \Cliente**, o **Explorador de Arquivos** pode ser encerrado inesperadamente.
- Tentativas de reconectar a uma sessão VDA podem falhar intermitentemente após a atualização para o Citrix Virtual Apps and Desktops versão 2203 LTSR ou 2203 LTSR CU1.
- Os VDAs podem apresentar uma exceção fatal em tdica.sys e exibir uma tela azul. O problema ocorre ao tentar reconectar-se a uma sessão.
- Os VDAs podem encontrar um código de verificação de bug, **000000CA**, se um dispositivo USB for inserido e removido rapidamente.
- As tentativas de habilitar SSL em VDAs podem falhar quando o modelo de certificado é criado com **Key Storage Provider** como provedor de **Criptografia**.
- O processo DllHost.exe pode ser encerrado inesperadamente com esta mensagem de erro:

  O COM Surrogate não está mais funcionando

- Durante o lançamento da sessão, os VDAs podem apresentar uma exceção fatal na Inicialização do Canal Virtual Personalizado do ControlUP e exibir uma tela azul.
- O Serviço de Redirecionamento de Vídeo HTML5 (CtxHdxWebSocketService) pode ser encerrado inesperadamente.
- O processo gráfico do software Citrix (Ctxgfx.exe) pode consumir memória não paginada excessiva nos VDAs, fazendo com que as máquinas virtuais se tornem sem resposta.
- Ao abrir um aplicativo publicado no modo minimizado ou em tela cheia, uma tela preta pode aparecer. O problema ocorre ao atualizar um VDA das versões 1912 LTSR para 2203 LTSR CU1 ou CU2.

Experiência do Usuário

- Várias tentativas de copiar conteúdo do aplicativo Microsoft Access podem falhar, pois o botão de colar no aplicativo é desativado.
- Ao fazer login pelo Citrix Gateway e o **LDAP SSO Name Attribute** estiver definido como **UserPrincipalName**, a marca d'água do Citrix pode exibir o nome de login incorretamente.

VDA para SO multissessão

Instalando, Desinstalando, Atualizando

- Com esta correção, a ferramenta VUA compara a versão principal ao realizar atualizações, permitindo atualizações de lançamento de CU. Agora você pode realizar atualizações LTSR como 2203.0.0.x para 2203.0.1000.x (CU1).

Teclado

- O teclado virtual pode não aparecer automaticamente em um aplicativo publicado ao posicionar o cursor em um campo editável.
- Ao abrir 2 instâncias de um aplicativo e definir a configuração **DisableToggler** para cinco segundos, pode ser necessário esperar cerca de 30 segundos antes de digitar no segundo aplicativo.

Impressão

- Em clientes Mac, o tamanho de papel padrão da impressora pode não ser retido depois que você faz logoff e logon novamente.

Sessão/Conexão

- O serviço CseEngine.exe pode consumir mais memória do que o esperado nos VDAs.
- Tentativas de imprimir um documento do Citrix Universal Print Server em impressoras de sessão compartilhada podem falhar. O problema ocorre após a atualização para o Citrix Virtual Apps and Desktops 1912 LTSR CU4.
- Ao iniciar um aplicativo de um VDA como usuário anônimo, esta mensagem de erro pode aparecer:

  Nome de usuário e senha incorretos.

- As tentativas de instalar um VDA versão 2203 podem falhar quando o sistema Windows não possui uma unidade C.

- Ao iniciar um desktop publicado, abrir o **Explorador de Arquivos** e clicar na unidade C local redirecionada em **Rede > \Cliente**, o **Explorador de Arquivos** pode ser encerrado inesperadamente.
- As tentativas de habilitar SSL em VDAs podem falhar quando o modelo de certificado é criado com **Provedor de Armazenamento de Chaves** como o provedor de **Criptografia**.
- O Citrix Director versão 2203 pode exibir detalhes da Sessão Interativa do lançamento do aplicativo publicado, como **Userinit** e **Shell**, em uma única linha em vez de linhas separadas.
- A operação de arrastar e soltar pode falhar ao passar o mouse de uma janela contínua para outra.
- Tentativas de compartilhar certos aplicativos personalizados usando o Microsoft Teams otimizado podem falhar.
- O serviço CtxRaveSvc.exe pode parar de responder e não receber notificações de alteração de sessão dos Serviços de Área de Trabalho Remota.
- O processo WebSocketService.exe pode consumir mais memória do que o esperado nos VDAs.
- Ao abrir um aplicativo publicado no modo minimizado ou tela cheia, uma tela preta pode aparecer. O problema ocorre ao atualizar um VDA da versão 1912 LTSR para as versões 2203 LTSR CU1 ou CU2.
- As máquinas em pool que estão LIGADAS podem ser desligadas automaticamente e se tornar não registradas. [

Exceções do Sistema

- O recurso de confiabilidade da sessão causa reconexões durante as quais o VDA pode apresentar exceções fatais e exibir uma tela azul.
- O serviço Citrix HDX RAVE (CtxSvcHost.exe) pode ser encerrado inesperadamente.
- O processo winlogon.exe do Microsoft Windows pode ser encerrado inesperadamente, causando o fechamento das sessões. O problema ocorre devido ao módulo icagfxstack.dll com falha ao atualizar um VDA da versão 1912 LTSR CU4 para 2203 LTSR.
- O processo do Terminal Services pode ser encerrado inesperadamente devido ao módulo com falha, RPM.dll.
- Os VDAs podem encontrar um código de verificação de bug, 000000CA, se um dispositivo USB for inserido e removido rapidamente.
- O processo DllHost.exe pode ser encerrado inesperadamente com esta mensagem de erro:

O COM Surrogate não está mais funcionando

- O processo do Host de Serviço (svchost.exe) pode consumir mais memória do que o esperado em um VDA para SO multi-sessão quando o componente UiPath Remote Runtime está instalado.
- Durante o lançamento da sessão, os VDAs podem apresentar uma exceção fatal na inicialização do Canal Virtual Personalizado do ControlUP e exibir uma tela azul.
- O serviço WebSocketAgent.exe pode ser encerrado inesperadamente ao tentar reproduzir um vídeo do YouTube com o redirecionamento de conteúdo do navegador ativado.
- O Serviço de Redirecionamento de Vídeo HTML5 (CtxHdxWebSocketService) pode ser encerrado inesperadamente.
- O processo gráfico do software Citrix (Ctxgfx.exe) pode consumir memória não paginada excessiva nos VDAs, fazendo com que as máquinas virtuais fiquem sem resposta.

Experiência do Usuário

- Várias tentativas de copiar conteúdo do aplicativo Microsoft Access podem falhar, pois o botão de colar no aplicativo é desativado.
- Ao fazer login no Citrix Gateway e o **Atributo de Nome SSO LDAP** estiver definido como **UserPrincipalName**, a marca d'água do Citrix pode exibir o nome de login incorretamente.

Componentes do Desktop Virtual – Outros

- Tentativas de iniciar um aplicativo App-V publicado podem falhar ao usar o modo de administrador duplo.
- As tentativas de iniciar aplicativos App-V podem falhar em máquinas não persistentes se o cache do App-V for redirecionado para a unidade persistente.

Citrix Provisioning™

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

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.

Atualização Cumulativa 2 (CU2)

Data de lançamento: December 08, 2022

Sobre esta versão

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 2 (CU2) corrige mais de 50 problemas relatados desde o lançamento do 2203 LTSR CU1.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

Novidades nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Aplicativos Virtuais e Desktops 7 2203 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 metainstaller do CU2. Antes de fazer isso, recomendamos que você se familiarize com o produto:

Examine a seção Citrix Virtual Apps and Desktops 7 2203 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 2203 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 2203 LTSR CU2

COMPONENTE DE LINHA DE BASE DO 2203 CU2	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.2000.2071	VDA de sessão única
VDA multissessão	2203.0.2000.2071	VDA multissessão
Delivery Controller	2203.0.2000.2071	Delivery Controller(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller)
Citrix Studio	7.33.2000.21	Citrix Studio(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/system-

COMPONENTE DE LINHA DE BASE DO 2203 CU2	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
		requirements.html#citrix-studio)
Citrix Director	7.33.2000.21	Citrix Director(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/director.html)
Citrix Group Policy Management	7.33.2000.12	Citrix Group Policy Management(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html)
Citrix Group Policy Client-Side Extension	7.33.2000.11	
Citrix StoreFront	2203.0.2000.5	Citrix StoreFront(/pt-br/storefront/)
Citrix Provisioning	2203.0.11	Provisionamento Citrix
Servidor de Impressão Universal	2203.0.2000.2066	Servidor de Impressão Universal
Gravação de Sessão	22.3.2000	Gravação de Sessão
Linux VDA	22.03.2000.5	Agente de Entrega Virtual Linux
Gerenciamento de Perfis	22.3.2000.1	Gerenciamento de Perfil
Serviço de Autenticação Federada Citrix	10.9.2000.9	Serviço de Autenticação Federada Citrix (FAS)
Redirecionamento de Conteúdo do Navegador	15.32.2000.1	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2206	2209.1.0.0	Baixar

Componentes compatíveis com 2203 LTSR CU2

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 apenas de correção). A Citrix® pode solicitar que você atualize para uma versão mais recente desses componentes em seus ambientes 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2208.0.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.500	HDX RealTime Optimization Pack
Servidor de Licenças	11.17.2.0 compilação 40000	Servidor de Licenças
Camada de personalização do usuário	22.6.3	Camada de personalização do usuário
Reprodutor web de Gravação de Sessão	22.3.2000.8	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32.1000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	2209	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa mais recente	Documentação

2203 LTSR CU2 exclusões notáveis

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. Especificamente, atualizações cumulativas e benefícios de ciclo de vida estendido estão excluídos. Atualizações para recursos e componentes excluídos estão disponíveis através de versões atuais regulares.

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

PLATAFORMAS WINDOWS EXCLUÍDAS *
Windows 2008 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.

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU1:

Política Citrix

- Uma consulta DNS incorreta pode ser gerada quando o CseEngine.exe está buscando um Objeto de Política de Grupo (GPO).

Citrix Studio

- Tentativas de criar um novo site do Citrix Virtual Apps and Desktops com as permissões **DBCreator**, **Securityadmin** e **Public permissions** a partir do console do Citrix Studio podem falhar.
- Esta correção oferece a capacidade de pesquisar um domínio ao criar um catálogo de máquinas. Para obter mais informações, consulte Criar catálogos de máquinas.
- Depois de navegar para **Delivery Group > Power management**, a tentativa de atualizar a barra de horários de pico pode falhar.

Delivery Controller™

- O Citrix Studio pode exibir Identificadores de Segurança (SID) de máquinas em vez de nomes de conta se alguns controladores de domínio estiverem desligados.

Gráficos

- Alguns aplicativos são limitados a uma taxa de quadros máxima de 22 quadros por segundo (FPS) em vez do máximo padrão de 30 FPS.

VDA para SO de sessão única

Sessão/Conexão

- Dois VDAs, em vez de um, podem ser atribuídos a um único usuário.
- Ao sair de uma sessão, o servidor pode parar de responder. O problema ocorre devido ao loop infinito presente em icausbb.sys.
- Ao iniciar um aplicativo publicado Citrix, o modo contínuo pode não ser ativado, resultando no aplicativo publicado com um fundo preto.
- Tentativas de reconfigurar VDA de SO multi-sessão executando o aplicativo Citrix Workspace™ para Windows versão 2203 podem falhar.
- Ao iniciar aplicativos da Plataforma Universal do Windows (UWP) como aplicativos hospedados em VM, o status do aplicativo **Aplicativo não em execução** é exibido.
- Com o recurso **Virtualization Based Security** ativado, ao acessar uma estação de trabalho usando o Acesso Remoto ao PC através de um dispositivo de usuário e, em seguida, desconectar, uma tela preta pode aparecer quando você fisicamente alcança a estação de trabalho e faz logon no sistema.
- Ao reconectar a um aplicativo publicado, dois aplicativos publicados podem ser iniciados e o Delivery Controller pode mostrar o estado do aplicativo como Aplicativo não em execução.
- Durante a reconexão da sessão, o indicador de status da bateria pode desaparecer se o cabo de alimentação estiver conectado.
- A extensão de redirecionamento de conteúdo do navegador pode falhar ao funcionar com a versão mais recente do Chrome, fazendo com que a chamada otimizada do Microsoft Teams seja desconectada.
- Com a versão mais recente do Chrome, a extensão de redirecionamento de conteúdo do navegador pode falhar e fazer com que a chamada otimizada do Microsoft Teams seja desconectada.

Exceções do Sistema

- O processo **ctxgfx** pode causar alto uso da CPU em VDA do Windows versão 2112 ao usar clientes Ubuntu 18 com monitores duplos.
- O Serviço de Redirecionamento de Áudio Citrix pode falhar ao funcionar com o VDA versão 2203.
- Os processos wfshell.exe ou PicaVcHost.exe podem ser encerrados inesperadamente com um código de exceção, 0xc0000374. O problema ocorre quando você define uma string longa na configuração da política URLs permitidas a serem redirecionadas para o cliente.
- O processo wfshell.exe pode ser encerrado inesperadamente devido ao módulo CtxUiMon.dll com falha.
- Se o Microsoft Azure Information Protection (AIP) estiver instalado e o Citrix Hook estiver ativado, os aplicativos do Microsoft 365 podem ser encerrados inesperadamente.

Experiência do Usuário

- Ao instalar o VDA versão 2203 em uma máquina Windows 11, o clique com o botão direito pode não funcionar no menu **Iniciar**.

VDA para SO multissessão

Sessão/Conexão

- Ao sair de uma sessão, o servidor pode parar de responder. O problema ocorre devido ao loop infinito presente em icausbb.sys.
- As tentativas de reconfigurar o VDA de SO multi-sessão executando o aplicativo Citrix Workspace para Windows versão 2203 podem falhar.
- A política 'Aplica-se às seguintes versões de VDA' listada em 'Nomes de impressoras cliente' mostra apenas o Virtual Delivery Agent 5.6 Feature Pack 1 como uma versão disponível.
- Com esta correção, novas configurações de usuário estão disponíveis para configurar sessões, temporizadores de inatividade e desconexão para VDAs multi-sessão. Para obter mais informações, consulte a documentação Configurações de política de limites de sessão.
- O protetor de tela pode aparecer em uma sessão reconectada de um aplicativo publicado contínuo através de um VDA que tem o protetor de tela ativado.
- Ao reconectar a um aplicativo publicado, dois aplicativos publicados podem ser iniciados e o Delivery Controller pode mostrar o status do aplicativo como 'Aplicativo não em execução'.

- Com esta correção, você pode usar curingas no caminho do processo ao adicionar canais virtuais à lista de permissões. Para obter mais informações, consulte a documentação Segurança do canal virtual.
- Durante a reconexão da sessão, o indicador de status da bateria pode desaparecer se o cabo de alimentação estiver conectado.
- Os VDAs podem parar de responder quando o RPM está retendo um processo de logoff por não liberar um bloqueio conforme o esperado.
- A extensão de redirecionamento de conteúdo do navegador pode falhar ao funcionar com a versão mais recente do Chrome, fazendo com que a chamada otimizada do Microsoft Teams seja desconectada.
- Com a versão mais recente do Chrome, a extensão de redirecionamento de conteúdo do navegador pode falhar e fazer com que a chamada otimizada do Microsoft Teams seja desconectada.

Exceções do Sistema

- Os VDAs podem apresentar uma exceção fatal em tdica.sys e exibir uma tela azul com um código de verificação de erro, 0x0000007E.
- Os VDAs podem apresentar uma exceção fatal em picavc.sys ou picadm.sys e exibir uma tela azul.
- O processo **ctxgfx** pode causar alto uso da CPU em VDAs Windows versão 2112 ao usar clientes Ubuntu 18 com monitores duplos.
- O processo wfshell.exe pode ser encerrado inesperadamente quando o canal virtual é desconectado.
- Os processos wfshell.exe ou PicaVcHost.exe podem ser encerrados inesperadamente com um código de exceção, 0xc0000374. O problema ocorre quando você define uma string longa na configuração da política URLs permitidas para serem redirecionadas para o cliente.
- O processo wfshell.exe pode ser encerrado inesperadamente devido ao módulo CtxUiMon.dll com falha.
- Ao tentar se conectar a um VDA executando a versão 2203 em um SO multi-sessão, o processo logonui.exe pode parar de responder com uma tela preta ou ser encerrado. No entanto, os logs de eventos podem aparecer.
- Os Serviços de Terminal em execução em um VDA de SO multi-sessão podem se desregistrar e sair intermitentemente.

Citrix Provisioning™

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

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.

Atualização Cumulativa 1 (CU1)

Data de lançamento: August 03, 2022

Sobre esta versão

A Atualização Cumulativa 1 foi relançada como Atualização Cumulativa 1100 em August 24, 2022. A nova versão aborda o problema LCM-11719, que, em alguns casos, impedia atualizações de VDA de sessão única para a Atualização Cumulativa 1 do 2203.

O Citrix Virtual Apps and Desktops™ 7 2203 LTSR Atualização Cumulativa 1 (CU1) corrige mais de 30 problemas relatados desde o lançamento inicial do 2203 LTSR.

2203 LTSR (informações gerais)

2203 LTSR (recursos e informações de atualização)

Novidades nesta versão

Problemas corrigidos no Citrix Virtual Apps and Desktops 7 2203 LTSR (lançamento inicial)

Problemas conhecidos nesta versão

Descontinuação e remoções

Datas de Elegibilidade do Citrix Product Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 2203 LTSR Atualização Cumulativa 1

Novas implantações

Como faço para implantar o CU1 do zero?

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

Examine a seção Citrix Virtual Apps and Desktops 7 2203 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 2203 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 2203 LTSR CU1

COMPONENTE DE LINHA DE BASE DO 2203 CU1	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.1100.1178	VDA de sessão única
VDA de múltiplas sessões	2203.0.1100.1178	VDA de múltiplas sessões

COMPONENTE DE LINHA DE BASE DO 2203 CU1	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
Delivery Controller	2203.0.1100.1178	Delivery Controller
Citrix Studio	7.33.1100.27	Citrix Studio
Citrix Director	7.33.1100.40	Citrix Director
Gerenciamento de Política de Grupo Citrix	7.33.1100.18	Gerenciamento de Política de Grupo Citrix
Extensão do Lado do Cliente da Política de Grupo Citrix	7.33.1100.16	
Citrix StoreFront	2203.0.1000.10	Citrix StoreFront
Citrix Provisioning	7.33.5	Citrix Provisioning
Servidor de Impressão Universal	7.33.1100.18	Universal Print Server
Gravação de Sessão	22.3.1100.1178	Session Recording
Linux VDA	22.03.1000.7	Linux Virtual Delivery Agent
Gerenciamento de Perfis	22.3.1000.4	Profile Management
Citrix Federated Authentication Service	10.9.1100.18	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.32.1100.9	Redirecionamento de Conteúdo do Navegador
Citrix Probe Agent 2206	2206.1.0.0	Baixar

Componentes compatíveis com 2203 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 2203.

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 compilação 39000	License Server
Camada de personalização do usuário	22.6.1	Camada de personalização do usuário
Reprodutor web de gravação de sessão	22.3.1000.5	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32.1000.9	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	2203.1.0.1	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa mais recente	Documentação

Exclusões notáveis do 2203 LTSR CU1

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. 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®
Citrix SCOM Management Pack
Framehawk

COMPONENTES E RECURSOS EXCLUÍDOS
Personal vDisk
StoreFront Citrix Online Integration

PLATAFORMAS WINDOWS EXCLUÍDAS *
Windows 2008 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

Não há novos recursos e aprimoramentos no Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 1 (CU1).

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2203 LTSR (versão inicial):

Citrix Director

- Após desinstalar um VDA, os namespaces para Citrix Windows Management Instrumentation (WMI) podem permanecer.
- As contagens de sessões ativas no Citrix Studio e no Citrix Director podem não corresponder.

Citrix Policy

- Os VDAs podem não se registrar com o Delivery Controller™ e permanecer não registrados.
- Tags ou Delivery Groups usados para atribuir políticas no Citrix Studio não podem ser enumerados além do limite de 250.

Citrix Studio

- Operações envolvendo catálogos de máquinas no Citrix Studio, como acessar, criar, remover ou enumerar catálogos, podem ser lentas. Esse problema ocorre se um hypervisor Nutanix for usado para hospedar a conexão.

Delivery Controller

- A atualização do Citrix Virtual Apps and Desktops para a versão 1912 LTSR pode não atualizar o arquivo de configuração Citrix.AzureRmPlugin.dll.config e a conexão com o Microsoft Azure Resource Manager pode falhar.
- Ao atualizar um catálogo do Machine Creation Services™, se você selecionar a máquina virtual e, em seguida, o snapshot relevante, esta mensagem de erro poderá aparecer:

  Ocorreu um erro inesperado. Entre em contato com o Suporte Técnico da Citrix.

- Tentativas de ligar uma máquina podem falhar depois que a conexão com o System Center Virtual Machine Manager (SCVMM) é restaurada.
- Ao usar um endereço IP estático para criar uma máquina VDA versão 2203 LTSR a partir de uma imagem mestre, o Machine Creation Services (MCS) pode não habilitar o DHCP durante a preparação da imagem.

VDA para SO de sessão única

Teclado

- O atalho de teclado **Ctrl+Break** pode não funcionar em sessões abertas usando o aplicativo Citrix Workspace™ para Linux.

Sessão/Conexão

- Ao conectar ou desconectar um monitor, a janela contínua pode ser posicionada incorretamente.
- O compartilhamento de certos aplicativos de terceiros usando o recurso de compartilhamento de tela no Microsoft Teams pode falhar.
- Ao tentar redimensionar a janela de um aplicativo compartilhado no Microsoft Teams, a borda vermelha que indica que o aplicativo está sendo compartilhado pode não corresponder ao tamanho real do aplicativo.
- Ao executar o Indicador de Qualidade da Conexão na versão 2112 do VDA, valores incorretos de Tempo de Ida e Volta (RTT) e latência podem ser relatados.

  Esta correção permite que você use a medição de latência NetScaler® L7 herdada quando o recurso HDX Adaptive Scaling estiver desabilitado. Os recursos de latência NetScaler L7 e HDX Adaptive Scaling do VDA não podem ser habilitados simultaneamente.

Para que a funcionalidade da correção entre em vigor, você deve desabilitar o recurso HDX™ Adaptive Scaling no registro do VDA da seguinte forma:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

Nome: AdaptiveScalingEnabled

Tipo: DWORD

Valor: 0

- Redimensionar uma janela do Desktop Viewer com a política de indicador de status gráfico ativada pode falhar e uma tela cinza pode aparecer momentaneamente. A tela cinza pode, às vezes, persistir até que você reinicie o VDA.
- Compartilhar certos aplicativos publicados usando o recurso de compartilhamento de tela no Microsoft Teams pode falhar.
- O Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) pode causar um vazamento de sessão ao usar o Microsoft Teams otimizado para Citrix HDX.
- As atualizações do VDA podem falhar quando o Citrix WEM Agent é instalado em uma máquina VDA sem informações de configuração.
- As atualizações do VDA de sessão única para o 2203 Cumulative Update 1 podem falhar e a seguinte mensagem de erro aparece:

  `IcaConfigConsole.exe failed with error code -4`

  Como solução alternativa, crie a seguinte chave de registro na máquina de destino antes da atualização:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

  Para obter mais informações, consulte o artigo da Central de Conhecimento CTX463588.

  Nota: Este problema foi resolvido no Cumulative Update 1100 - a nova versão do Cumulative Update 1.

Exceções do Sistema

- O processo wfshell.exe pode ser encerrado inesperadamente, fazendo com que novos lançamentos de aplicativos publicados falhem.

- Um erro no CTXCDF pode fazer com que o Serviço de Provedor de Instrumentação de Gerenciamento do Windows (WMIPRVSE.exe) pare e gere o ID de Evento 5612 no log de eventos.
- O processo WebSocketService.exe pode ser encerrado inesperadamente, fazendo com que as chamadas do Microsoft Teams falhem com a seguinte mensagem de erro:

  Ainda conectando a dispositivos remotos. A chamada ainda não está disponível.

- O processo PicaVcHost.exe pode apresentar uma violação de acesso e ser encerrado inesperadamente.

Experiência do Usuário

- Um mouse para canhotos com o botão principal definido como **Esquerdo** no dispositivo do usuário e no VDA pode não funcionar como esperado.

Interface do Usuário

- Fornecer controle de tela a outro usuário ao usar o recurso de Compartilhamento de Tela pode causar um prompt de tradução chinesa incorreto, **`<xxx>` quer visualizar sua área de trabalho para aparecer em vez de `<xxx>` quer controlar sua área de trabalho**.

VDA para SO multi-sessão

Sessão/Conexão

- Os seguintes problemas de aplicativos publicados HDX foram resolvidos:
  - O prompt de senha do Microsoft Office pode não aparecer.
  - Dispositivos como **Impressoras e Scanners** podem não aparecer no menu **Configurações**.
  - Pastas recém-criadas podem não aparecer no aplicativo **Explorador de Arquivos**.
  - **Abrir Configurações** no menu **Explorador de Arquivos** não funciona.
  - Em aplicativos como Microsoft Word ou Microsoft Excel, ao renomear, criar ou excluir uma pasta usando a opção **Salvar** ou **Abrir**, a janela não é atualizada automaticamente. No entanto, você pode atualizar a janela manualmente.
  - Durante o lançamento de um aplicativo Universal Windows Platform (UWP), o aplicativo aparece na tela 8-13 segundos depois que a barra de progresso de conclusão da sessão do aplicativo Citrix Workspace desaparece. Como resultado, os usuários podem tentar fazer vários lançamentos.

- Em uma sessão HDX contínua no Windows 11 versão 22H2, a janela de impressão pode ser exibida parcialmente se uma caixa de diálogo de Impressão estiver aberta.
- A barra de pesquisa do **Explorador de Arquivos** não funciona.
- Aplicativos Universal Windows Platform (UWP) não podem ser iniciados com sucesso se um aplicativo não-UWP tiver sido iniciado antes.
- Quando aplicativos do Microsoft Office 365 build 16.0.7967 e posteriores são publicados como aplicativos de um host Windows Server 2019, a ativação da licença do Office falha.

Para habilitar a correção, siga os seguintes passos:

- Adicione os seguintes detalhes de registro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  Nome: Shellbridge

  Tipo: REG_DWORD

  Valor: 1
- Certifique-se de que a seguinte atualização do SO esteja instalada:

  Windows 11: KB5014019

  Windows Server 2022: KB5014021

  Windows 10: KB5014023

  Windows Server 2019: KB5014022

- A permissão do TermService na chave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Session pode não ser restaurada durante a instalação de um VDA no Citrix Virtual Apps and Desktops 1912 CU, resultando em falhas de sessão.
- Ao executar o Indicador de Qualidade de Conexão na versão 2112 do VDA, valores incorretos de Round Trip Time (RTT) e latência podem ser relatados.

  Esta correção permite usar a medição de latência NetScaler L7 legada quando o recurso HDX Adaptive Scaling está desabilitado. Os recursos de latência NetScaler L7 e HDX Adaptive Scaling do VDA não podem ser habilitados simultaneamente.

Para que a funcionalidade da correção entre em vigor, você deve desabilitar o recurso HDX Adaptive Scaling no registro do VDA da seguinte forma:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

Nome: AdaptiveScalingEnabled

Tipo: DWORD

Valor: 0

- A política **Aplica-se às seguintes versões de VDA**, listada em **Nomes de impressoras cliente**, mostra apenas o Virtual Delivery Agent 5.6 Feature Pack 1 como uma versão disponível.
- Tentativas de reconectar a uma sessão podem falhar e a sessão pode desaparecer do Citrix Director. Uma nova sessão é iniciada em vez de reconectar à sessão existente. Para habilitar a correção, defina a seguinte chave de registro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  Nome: EnforceUserPolicyEvaluationSuccess

  Tipo: REG_DWORD

  Valor: 0

- As atualizações do VDA podem falhar quando o Citrix WEM Agent é instalado em uma máquina VDA sem informações de configuração.

Exceções do Sistema

- O processo wfshell.exe pode ser encerrado inesperadamente, fazendo com que novos lançamentos de aplicativos publicados falhem.
- Um erro no CTXCDF pode fazer com que o Serviço de Provedor de Instrumentação de Gerenciamento do Windows (WMIPRVSE.exe) pare e gere o ID de Evento 5612 no log de eventos.
- O processo wfshell.exe pode ser encerrado inesperadamente quando o canal virtual é desconectado.
- O Explorador de Arquivos pode ser encerrado inesperadamente ao fechar a janela **Abrir Configurações**.

- O Serviço de Terminal pode ser encerrado intermitentemente no VDA para SO de múltiplas sessões. O ID de Evento 7011 é registrado no log de eventos do Sistema com a seguinte mensagem:

  Um tempo limite (30000 milissegundos) foi atingido enquanto aguardava uma resposta de transação do serviço TermService.

Experiência do Usuário

- Um mouse para canhotos com o botão principal definido como **Esquerdo** no dispositivo do usuário e no VDA pode não funcionar como esperado.

Interface do Usuário

- Arrastar e soltar arquivos entre a sessão Citrix e o endpoint local pode falhar mesmo que a política de **Arrastar e Soltar** esteja habilitada. Um erro pop-up **CtxDnDSourceProxy** aparece.

Componentes do Desktop Virtual – Outros

- Tentativas de iniciar aplicativos App-V podem falhar em máquinas não persistentes se o cache do App-V for redirecionado para a unidade persistente.

Citrix Provisioning™

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

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.

2203 LTSR (versão inicial)

Sobre esta 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 1912 e XenApp and XenDesktop Versão 7.15.

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

- **Instalar ou atualizar um site:** Use o ISO desta versão para instalar ou atualizar os componentes principais e os 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.

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

Para instruções de instalação e atualização:

- Se você estiver criando 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 2203 LTSR

COMPONENTE DE LINHA DE BASE 2203	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
VDA de sessão única	2203.0.0.33220	VDA de sessão única
VDA multissessão	2203.0.0.33220	VDA multissessão
Delivery Controller	2203.0.0.33220	Delivery Controller
Citrix Studio	7.33.0.70	Citrix Studio
Citrix Director	7.33.0.67	Citrix Director
Gerenciamento de Política de Grupo Citrix	7.33.0.33	Gerenciamento de Política de Grupo Citrix
Extensão do Lado do Cliente da Política de Grupo Citrix	7.33.0.22	
Citrix StoreFront	2203.0.0.36	Citrix StoreFront
Citrix Provisioning	2203.0.0	Citrix Provisioning
Servidor de Impressão Universal	7.33.0.12	Servidor de Impressão Universal
Gravação de Sessão	22.3.0	Gravação de Sessão
Linux VDA	22.03.0.16	Agente de Entrega Virtual Linux
Gerenciamento de Perfis	22.3.0.7	Gerenciamento de Perfis
Serviço de Autenticação Federada Citrix	10.9.0.23	Serviço de Autenticação Federada Citrix (FAS)
Redirecionamento de Conteúdo do Navegador	15.32.0.17	Redirecionamento de Conteúdo do Navegador
Agente de Sondagem Citrix	2103.1.0.0	Baixar

Componentes compatíveis com a versão inicial 2203 LTSR

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 2203.

COMPONENTES E RECURSOS COMPATÍVEIS	VERSÃO CONFORME EXIBIDO EM PROGRAMAS E RECURSOS	DOCUMENTAÇÃO
App Layering	2202.0.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.400	HDX RealTime Optimization Pack
Servidor de Licenças	11.17.2.0 compilação 37000	Servidor de Licenças
Camada de personalização do usuário	21.12.5.7	Camada de personalização do usuário
Reprodutor web de Gravação de Sessão	22.3.0.24	Reprodutor web de gravação de sessão
Otimização do Microsoft Teams	15.32	Otimização do Microsoft Teams
Gerenciamento do Ambiente de Trabalho	2203.1.0.1	Gerenciamento do Ambiente de Trabalho
XenApp & XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente a Atualização Cumulativa Mais Recente	Documentação

Exclusões notáveis da versão inicial 2203 LTSR

Os seguintes recursos, componentes e plataformas não são elegíveis para os marcos e benefícios do ciclo de vida 2203. Especificamente, as atualizações cumulativas e os benefícios de ciclo de vida estendido estão 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
Integração do StoreFront Citrix Online

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

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

O que há de novo

Este artigo lista os recursos novos e aprimorados para Citrix Virtual Apps and Desktops™ 7 2203 LTSR (versão inicial). As atualizações são organizadas por componente.

Comandos PowerShell para gerenciar o Local Host Cache (LHC)

Agora você pode usar comandos PowerShell para gerenciar o LHC nos Delivery Controllers. Para obter mais informações, consulte Comandos PowerShell do Local Host Cache.

Licença de Direitos Híbridos

A partir da versão inicial 2203 LTSR, as conexões de host de nuvem pública anteriormente não suportadas agora podem ser implantadas usando a nova **Licença de Direitos Híbridos**. Assim, agora você pode usar implantações locais com implantações em nuvem. As conexões de host de nuvem pública suportadas são: AWS, Azure e Google Cloud. Se sua implantação tiver conexões de host de nuvem pública, você não poderá atualizar para a versão atual sem a Licença de Direitos Híbridos. Para obter mais informações, consulte o seguinte:

- Transição e Upgrade (TTU) com Direitos Híbridos
- Atualizar uma implantação

- Citrix Provisioning
- Requisitos do Sistema

Virtual Delivery Agents (VDAs) 2203

A versão 2203 dos VDAs de SO de sessão única e SO de múltiplas sessões do Windows inclui os seguintes aprimoramentos. Esses itens são adicionais a quaisquer itens de instalação e atualização de VDA listados anteriormente neste artigo.

Aprimoramentos de layout de teclado para a tela de login do Windows

A versão inicial 2203 LTSR aborda problemas de layout de teclado que ocorrem na tela de login do Windows solicitada por um VDA quando o logon único não é possível (por exemplo, durante um lançamento baseado em concessão de conexão ao usar a Continuidade do Serviço). Antes desta versão, o layout de teclado do VDA era usado na tela de login do Windows.

A partir da versão inicial 2203 LTSR, ao fazer login em uma sessão virtual no VDA, agora você pode inserir credenciais usando o layout de teclado do seu cliente local.

Atualização de áudio adaptável

O áudio adaptável e o áudio UDP agora têm uma nova implementação. Para obter mais informações, consulte Transporte de áudio UDP em tempo real e intervalo de porta UDP de áudio.

Citrix Director

Suporte a TLS 1.3

O Citrix Director agora oferece suporte à versão 1.3 do TLS.

Citrix Studio

Alterações no suporte a host para versões atuais

A partir da versão inicial 2203 LTSR, as versões atuais do produto oferecem suporte a VDAs (máquinas que fornecem aplicativos e desktops) nos seguintes hosts de nuvem pública:

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure Resource Manager

> **Importante:**

> Se você quiser adicionar conexões de host de nuvem pública à sua implantação, você precisa de uma Licença de Direitos Híbridos. Para obter informações sobre a Licença de Direitos Híbridos, consulte Transição e Upgrade (TTU) com Direitos Híbridos.

> Para obter uma lista completa de hosts e recursos de virtualização compatíveis, consulte Requisitos do sistema.

Verificações de validade da licença

O Citrix Studio agora verifica automaticamente a validade das licenças em uso pelas conexões de host. Uma conexão de host é colocada em modo de manutenção se sua licença for inválida. Como resultado, você não pode realizar certas operações, como editar a conexão e desativar o modo de manutenção. Uma licença se torna inválida, por exemplo, quando:

- A licença expirou. Nesse caso, entre em contato com seu representante de vendas da Citrix para renová-la ou para adquirir novas licenças.
- A licença foi excluída do Servidor de Licenças.

Citrix Provisioning™ versão inicial 2203 LTSR

A versão inicial do Citrix Provisioning 2203 LTSR contém novos recursos e correções.

Versão inicial do Linux Virtual Delivery Agent 2203 LTSR

A versão inicial do Linux Virtual Delivery Agent 2203 LTSR contém novos recursos e correções.

Versão inicial do Profile Management 2203 LTSR

A versão inicial do Profile Management 2203 LTSR contém novos recursos e correções.

Versão inicial do Session Recording 2203 LTSR

A versão inicial do Session Recording 2203 LTSR contém novos recursos e nenhuma correção.

Versão inicial do StoreFront™ 2203 LTSR

A versão inicial do StoreFront 2203 LTSR contém novos recursos e correções.

Workspace Environment Management™ 2203

O Workspace Environment Management 2203 contém novos recursos e correções.

Problemas corrigidos

Os seguintes problemas foram corrigidos desde o Citrix Virtual Apps and Desktops™ 7 2112:

Otimização do Microsoft Teams

- Quando mais de 1000 janelas de aplicativos estão abertas, a enumeração de compartilhamento de aplicativos falha e nenhum aplicativo é listado na bandeja de compartilhamento.

VDA para SO de sessão única

Teclado

- Em um dispositivo Android conectado a um VDA executando a versão 1912 LTSR CU3, ao ativar um campo de entrada de texto, o teclado na tela pode não aparecer automaticamente.
- Ao iniciar sessões de usuário, o Editor de Método de Entrada (IME) genérico do cliente pode não ser definido automaticamente. Como resultado, o teclado não sincroniza automaticamente com o endpoint.
- Esta correção aborda problemas de mapeamento de teclado russo no aplicativo Citrix Workspace™ para clientes HTML5, Mac e Linux.

Impressão

- Quando o redirecionamento de impressora cliente está habilitado em um desktop publicado, algumas configurações da impressora cliente podem não sincronizar com as configurações da impressora no VDA.
- As impressoras de sessão podem desaparecer durante a reconexão da sessão, tornando os VDAs inacessíveis a partir de um Remote Desktop (RDP).

Sessão/Conexão

- Ao sair de uma sessão, o servidor pode parar de responder. O problema ocorre ao usar o redirecionamento USB Genérico.
- As seguintes etapas, realizadas em um aplicativo Microsoft Outlook publicado com o IME local habilitado, podem levar a uma string aleatória inserida na janela de e-mail:
    - Abra a janela de e-mail.
    - Pressione a tecla Esc para exibir a caixa de diálogo **Deseja salvar suas alterações?** e digite um texto aleatório.
    - Pressione a tecla Esc para fechar a caixa de diálogo.
- Quando o Citrix IME está ativado, certos aplicativos de terceiros podem não responder e os lançamentos de aplicativos em uma sessão de usuário podem falhar. O problema ocorre devido ao módulo CtxIme com falha.

Exceções do Sistema

- Os VDAs podem apresentar uma exceção fatal e exibir uma tela azul com o código de verificação de erro 0x0000010D (WDF_VIOLATION).
- Ao atualizar seu VDA para a versão 2009 ou posterior, os erros de falha do Kernelbase (KERNELBASE.dll) podem aparecer nos logs de eventos. O problema ocorre com os navegadores Google Chrome e Microsoft Edge.

Interface do Usuário

- Em um ambiente de vários monitores, se você definir o monitor principal para o modo retrato, as notificações SAS podem aparecer giradas em 90 graus.

Experiência do Usuário

- Um mouse para canhotos com o botão principal definido como **Esquerdo** no dispositivo do usuário e no VDA pode não funcionar como esperado.

VDA para SO multissessão

Teclado

- Em um dispositivo Android conectado a um VDA executando a versão 1912 LTSR CU3, quando você ativa um campo de entrada de texto, o teclado na tela pode não aparecer automaticamente.

Impressão

- Quando o redirecionamento de impressora cliente está habilitado em um desktop publicado, algumas configurações da impressora cliente podem não sincronizar com as configurações da impressora no VDA.
- As impressoras de sessão podem desaparecer durante a reconexão da sessão, tornando os VDAs inacessíveis a partir de um Remote Desktop (RDP).

Sessão/Conexão

- Definir o valor de **HideStatusMessages** como 1 para ocultar a barra de inicialização pode fazer com que a chave do Registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ não funcione como esperado.
- Certos aplicativos de terceiros podem parar de responder em uma sessão contínua.
- Ao sair de uma sessão, o servidor pode parar de responder. O problema ocorre ao usar o redirecionamento USB Genérico.

- Quando o Citrix IME está ativado, certos aplicativos de terceiros podem não responder e os lançamentos de aplicativos em uma sessão de usuário podem falhar. O problema ocorre devido ao módulo CtxIme com falha.
- Quando as licenças se esgotam no License Server e o recurso **Modo de intermitência de licença** está desativado, uma tela preta congelada com a mensagem de erro **Acesso Negado** pode aparecer.
- Com o EDT como protocolo de transporte, os dispositivos do usuário podem ser desconectados do VDA devido à instabilidade da rede. Quando a rede é restaurada, a reconexão ao VDA leva muito tempo.
- Ao sair de uma sessão virtual do Citrix, um ou mais dos seguintes problemas podem ocorrer:
  - O VDA ainda lista a sessão encerrada e o processo logonui.exe. O processo logonui.exe pode ser encerrado à força.
  - A sessão aparece com um nome de usuário em branco no Citrix Studio.
  - Você pode não conseguir iniciar mais sessões.

Exceções do Sistema

- Quando você inicia a Conexão de Área de Trabalho Remota (mstsc.exe) como um aplicativo publicado, o processo CredentialUIBroker.exe pode ser encerrado inesperadamente.
- O Serviço de Controle de Pilha do Citrix (SCService64.exe) pode ser encerrado inesperadamente.
- Ao atualizar seu VDA para a versão 2009 ou posterior, os erros de falha do Kernelbase (KERNELBASE.dll) podem aparecer nos logs de eventos. O problema ocorre com os navegadores Google Chrome e Microsoft Edge.

Citrix Provisioning™

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

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.

Problemas conhecidos

Notas

- Problemas conhecidos descritos nas seções 2203 da versão inicial, CU1, CU2, CU3 e CU4 deste artigo continuam presentes no CU5, 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 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.

Problemas conhecidos no 2203 CU7

- Se você atualizar do 2203 LTSR CU7 para o 2402 LTSR CU1 ou CU2, versões anteriores e incluindo 2411, a atualização poderá falhar. Como solução alternativa, você pode atualizar diretamente para uma versão mais recente, como 2402 LTSR CU3/ CVAD 2503 ou posterior.

- A criação de uma nova conexão de host AWS/Azure em um site parcialmente atualizado pode falhar. Recomenda-se criar uma nova conexão de host em um site totalmente atualizado.
- 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 reproduzem automaticamente, embora estejam disponíveis.

Problema conhecido no 2203 CU6

- O suporte a FIDO2 não está disponível para o navegador Firefox de 32 bits nesta versão.

Problema conhecido no 2203 CU5

- Quando você já tem o aplicativo Citrix Workspace versão 22.03.5000 instalado (que está disponível no Citrix Virtual Apps and Desktops 2203 CU4 VDA e CU4 Update 1) e tenta atualizar para a versão mais recente, a atualização pode falhar devido a um pop-up de atualização automática. Use as seguintes soluções alternativas antes de atualizar o VDA para CU5:

  a. Atualize para o aplicativo Citrix Workspace versão 2203.1 LTSR CU6 ou aplicativo Citrix Workspace 2402 LTSR.

  b. Desative a atualização automática. Para obter mais informações, consulte Configurar atualizações do Citrix Workspace usando o modelo administrativo de Objeto de Política de Grupo.

  c. Selecione **Lembrar-me mais tarde** para o prompt de atualização do aplicativo Citrix Workspace™.

Problemas conhecidos no 2203 CU4

- Se você instalar o Windows, o IIS e o Citrix Director em unidades diferentes de C:\ e atualizar o Citrix Director para a versão 2203 LTSR CU4, o ícone do Citrix Director poderá aparecer em branco. No entanto, você pode clicar no ícone para iniciar o Citrix Director.

  Você pode usar a seguinte solução alternativa para ajudar a exibir o ícone corretamente.

1. Abra o prompt de comando e execute o comando echo **%systemdrive%**.
2. Copie a saída do comando.

3. Clique com o botão direito do mouse no ícone do Citrix Director > Mais > Abrir local do arquivo.
4. Abra o Bloco de Notas e arraste o ícone do explorador de arquivos para o Bloco de Notas.
5. No conteúdo, substitua “C:” pela saída copiada na etapa 2 e salve.
6. O ícone do Citrix Director agora será exibido corretamente.

- A tentativa de iniciar a enumeração de recursos ou aplicativos pode falhar ao atualizar o StoreFront™ para a versão 2203 LTSR CU4.

  > **Observação:**
  >
  > O problema foi corrigido na atualização 1 do 2203 LTSR CU4.

- Os VDAs podem apresentar uma exceção fatal em picadd.sys e exibir uma tela azul com o código de verificação de erro 0x96.

  > **Observação:**
  >
  > O problema foi corrigido na atualização 1 do 2203 LTSR CU4.

Problemas conhecidos no 2203 CU3

- Alguns dispositivos de áudio podem ser listados com um nome incorreto na lista de dispositivos.
- As tentativas de instalar o aplicativo Citrix Workspace junto com a instalação do VDA podem falhar se não houver acesso à internet. Como solução alternativa, você deve ignorar a instalação do aplicativo Citrix Workspace ou instalar o Microsoft WebView (que é um pré-requisito para o aplicativo Citrix Workspace) antes de instalar o VDA.

Problemas conhecidos no 2203 CU2

- As tentativas de instalar o aplicativo Citrix Workspace junto com a instalação do VDA podem falhar se não houver acesso à internet. Como solução alternativa, você deve ignorar a instalação do aplicativo Citrix Workspace ou instalar o Microsoft WebView (que é um pré-requisito para o aplicativo Citrix Workspace) antes de instalar o VDA.

- As tentativas de atualizar o Session Recording do Citrix Virtual Apps and Desktops™ 2203 LTSR CU1 para CU2 podem falhar. Esta mensagem de erro aparece:

  Não foi possível concluir a instalação.

  A instalação não foi concluída porque ocorreu um problema durante a inicialização. O produto funcionará, mas o desempenho poderá ser reduzido.

- O Profile Management pode redefinir o caminho OST personalizado do Outlook durante o logon.

Problemas conhecidos no 2203 CU1

- As tentativas de instalar o aplicativo Citrix Workspace junto com a instalação do VDA podem falhar se não houver acesso à internet. Como solução alternativa, você deve ignorar a instalação do aplicativo Citrix Workspace ou instalar o Microsoft WebView (que é um pré-requisito para o aplicativo Citrix Workspace) antes de instalar o VDA.
- Os VDAs podem apresentar uma exceção fatal em tdica.sys e exibir uma tela azul com um código de verificação de erro, 0x0000007E.

Problemas conhecidos na versão inicial 2203

Geral

- 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.
- Após a instalação do plug-in do aplicativo Web do Skype for Business, as webcams podem não ser enumeradas e as páginas de reunião no Firefox podem não ser atualizadas automaticamente.
- Ao iniciar um aplicativo do StoreFront, o aplicativo pode não iniciar em primeiro plano, ou o aplicativo está em primeiro plano, mas pode não ter foco. Como solução alternativa, clique no ícone na barra de tarefas para trazer o aplicativo para a frente ou na tela do aplicativo para trazê-lo para o foco.
- Ao usar o Windows 10 1809 LTSC, as dependências `VCLibs` falham ao instalar.

- 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.
- Você ativou o Acesso a Aplicativos Locais. Se você iniciar uma sessão VDA do Windows 2012 R2, desconectar e reconectar a sessão e, em seguida, iniciar um aplicativo local e maximizá-lo, a barra de tarefas do VDA poderá truncar o aplicativo.
- Em ambientes Azure, ao fazer login no VDA usando a sessão ICA®, você pode ver uma tela preta por aproximadamente cinco minutos se iniciar um aplicativo seamless para o mesmo desktop.
- O Citrix Hypervisor™ não oferece suporte a VMs de clone completo do MCS com SRs GFS2.
- 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.
- Quando aplicativos do Microsoft Office 365 build 16.0.7967 e posterior são publicados como aplicativos de um host Windows Server 2019, a ativação da licença do Office falha. A Citrix está trabalhando com a Microsoft para resolver essa limitação da Microsoft. A solução alternativa suportada é instalar VDAs do Windows Server 2016, que não possuem o componente Web Authentication Manager que está se comportando mal.
- O Gerenciador de Sessões encerra os inícios de sessão quando a avaliação da Política de Grupo falha. Isso é para evitar o acesso do usuário a recursos que são restritos por meio da Política de Grupo. A seguinte correção implementada pelo usuário fornece uma alternância de registro para que os administradores dispensem a aplicação, o que ajuda os usuários finais a se conectarem às sessões mesmo que a avaliação da Política de Grupo falhe:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  Nome: EnforceUserPolicyEvaluationSuccess

  Tipo: REG_DWORD

  Valor: 0 (ativa a correção atual)

- O Serviço de Terminal em execução em um VDA de SO multi-sessão pode ser encerrado intermitentemente. O ID do Evento 7011 é registrado no log de Eventos do Sistema com a seguinte mensagem:

Um tempo limite (30000 milissegundos) foi atingido enquanto aguardava uma resposta de transação do serviço TermService.

- Seus dispositivos de áudio High Definition Experience (HDX) são desativados ao se conectar a um RemotePC de sessão única ou Virtual Delivery Agent (VDA) de Workstation em um cliente que está habilitando mais de oito dispositivos de áudio HDX. Como solução alternativa, escolha uma das seguintes opções:
  - Conecte-se a um RemotePC de sessão única ou VDA de Workstation a partir de um cliente que esteja habilitando menos de oito dispositivos de áudio HDX.
  - Habilite os dispositivos de áudio HDX depois que o RemotePC de sessão única ou o VDA de Workstation for iniciado.
  - Conecte-se a um RemotePC de várias sessões ou VDA de Workstation.
- Os VDAs podem apresentar uma exceção fatal em tdica.sys e exibir uma tela azul com um código de verificação de erro, 0x0000007E.
- Em alguns cenários, ao usar o filtro de política de IP do Cliente, o endereço IP usado para avaliar a política está incorreto.

Studio

- 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.

Director

- O link **Console** em **Citrix Director > Detalhes da Máquina** não inicia o console da máquina nos navegadores Microsoft Edge 44 e Firefox 68 ESR.

Gráficos

- Ao compartilhar um aplicativo minimizado, a barra de título do aplicativo também pode ser compartilhada.
- Definir a política **Exibir conteúdo da janela ao arrastar** como **Proibido** não funciona no ESXi e no Hyper-V.
- Se você iniciar uma pré-visualização de vídeo usando um aplicativo de webcam de 64 bits com compactação Theora, a sessão poderá travar.

- Alguns aplicativos são limitados a uma taxa de quadros máxima de 22 quadros por segundo (FPS) em vez do máximo padrão de 30 FPS. Uma correção estará disponível no 2203 LTSR CU2. Como solução alternativa, defina o seguinte valor de registro no VDA:
  - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
  - Valor: EnableTimerPeriod = 1

  Para ativar a configuração, você deve desconectar e reiniciar a sessão.

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 Server 2012, Windows 10 e Windows 8. Para obter mais informações, consulte CTX213540.
- A impressora padrão pode não estar marcada corretamente na janela de diálogo de impressão. Esse problema não afeta os trabalhos de impressão enviados para a impressora padrão.

Machine Creation Services™ (MCS)

- Em ambientes GCP, quando você atualiza a propriedade personalizada de um esquema de provisionamento, as alterações não se aplicam às máquinas recém-adicionadas em um catálogo. Para resolver esse problema, após atualizar a propriedade personalizada de um esquema de provisionamento, crie uma nova imagem atualizada para o catálogo.
- Ao criar um catálogo com propriedades personalizadas, e usar `Set-ProvScheme` para alterar o esquema de provisionamento sem atualizar as mesmas propriedades personalizadas definidas durante a criação do catálogo, as propriedades que não são mencionadas em `Set-ProvScheme` são definidas para seus valores padrão. Além disso, se você definir qualquer propriedade personalizada para seu valor não padrão durante a criação do catálogo, ela será substituída por seu valor padrão após executar `Set-ProvScheme`.

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`.

- Na redireção de conteúdo do navegador, após iniciar um vídeo do YouTube usando o reprodutor de vídeo HTML5 do YouTube, o modo de tela cheia pode não funcionar. Você clica no ícone no canto inferior direito do vídeo, e o vídeo não redimensiona, deixando o fundo preto em toda a área da página. Como solução alternativa, clique no botão de tela cheia e selecione o modo teatro.

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 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

Os itens descontinuados não são removidos imediatamente. A Citrix continua a suportá-los, mas eles serão removidos em uma versão futura.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
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

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			que usam licenciamento 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 Citrix locais após April 15, 2026.
Suporte para formato WebRTC SDP (Plano B)	2308	---	Atualize o Citrix Workspace™ App para uma versão compatível.
Suporte para 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.
Importar dispositivos de destino do Citrix Provisioning para catálogos do Citrix Virtual Apps and Desktops™ para gerenciamento	1912 LTSR	-	Use o Assistente de Exportação de Dispositivos do Citrix Provisioning.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Redirecionamento de Host para Cliente (URL)	2203	---	---
Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress` usados em ambientes de nuvem e locais.	2203		
Citrix Files 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 autônomo Wake on LAN.
Citrix SCOM Management Packs para XenApp e XenDesktop,	1912		Use o Director para monitorar e gerenciar sua implantação. Para

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Provisioning Services e StoreFront. Para as versões de produto que podem ser monitoradas, consulte a documentação dos Citrix SCOM Management Packs.			obter mais informações sobre o EOL do SCOM e alternativas, consulte https://support.citrix.com/article/CTX266943.
SDK de Mobilidade / SDK Móvel (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
Console de Administração de Licenças Citrix (última vez incluído 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.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte ao adaptador gráfico Citrix Indirect Display Driver (IDD) no Windows 10 versão 1709 e anteriores.	2003	2003	Use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR.
Codificação de hardware com GPUs Nvidia (NVENC) usando drivers de vídeo GRID 9 ou anteriores.	2003	2003	Use drivers de vídeo GRID 10 com VDAs do Citrix Virtual Apps and Desktops 7 2003 ou posterior, ou use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR.
Recurso de Redefinição de Senha de Autoatendimento (SSPR).	2003	2006	
Suporte para versões do Microsoft .NET Framework anteriores à versão 4.8 para VDAs e componentes principais do servidor. Inclui Delivery Controller, Studio, Director e StoreFront.	1912	2003	Atualize para o .NET Framework versão 4.8.
VDAs no Windows Server 2012 R2.	1912	2003	Instale VDAs em um sistema operacional compatível.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Componente de migração de aplicativos AppDNA® da edição Premium do Citrix Virtual Apps and Desktops.	1909	2003	
Instalando o Studio em máquinas de 32 bits (x86).	1909	2003	Instale em um sistema operacional x64 compatível.
Suporte para o 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 Service Packs). Inclui: Delivery Controller™, Studio e Director.	1906	2003	Instale em um sistema operacional mais recente e compatível.
Suporte para bancos de dados de Configuração de Site, Registro de Configuração e Monitoramento nas versões 2008 R2,	1906	2003	Instale bancos de dados em uma versão compatível do Microsoft SQL Server.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
2012 e 2014 do Microsoft SQL Server (incluindo todos os Service Packs e edições).			
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 descontinuados no StoreFront: VDI-in-a-Box e XenMobile (9.0 e anteriores).	1903	1903	
Suporte para Linux VDA no Red Hat Enterprise Linux/ CentOS 7.5.	1903	1903	Instale o Linux VDA em uma versão posterior do Red Hat Enterprise Linux.
Suporte do StoreFront para os protocolos TLS 1.0 e TLS 1.1 entre Citrix	7.17	2203	Atualize os Citrix Receivers para um aplicativo Citrix Workspace que

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) e Citrix Receiver, e Workspace Hub.			suporte o protocolo TLS 1.2. Para obter mais informações sobre o aplicativo Citrix Workspace, consulte https://docs.citrix.com/pt-br/citrix-workspace-app.
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 remoto de exibição Framehawk	1811	1903	Use Thinwire com transporte adaptável ativado.
Suporte para Citrix Smart Scale em todas as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Esta funcionalidade atingirá o Fim da Vida em 31 May 2019.	1808	1906	Considere usar o Virtual Apps and Desktops Service no Citrix Cloud para 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	7.18	1808	Atualize para a versão 4.7.1 ou posterior do .NET Framework. (O instalador instala automaticamente o .NET Framework

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
e Citrix Delivery Controller.			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 do VDA para a configuração de política "Instalação automática de drivers de impressora integrados".	7.16	7.16	Nenhum. Configuração de política suportada apenas com VDAs em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores).
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 driver Citrix WDDM em VDAs	7.16	7.16	O driver Citrix WDDM não é mais instalado com VDAs.
VDAs no Windows 10 versão 1511 (Threshold 2) e versões anteriores do Windows Single-session OS, incluindo Windows 8.x e Windows 7 (consulte `<https://www.citrix.com/blogs/2018/01/08/`	7.15 LTSR (e 7.12)	7.16	Instale VDAs de SO de sessão única no Windows 10 versão mínima 1607 (Redstone 1) ou Canais Semestrais mais recentes. Se estiver usando 1607 LTSB, recomendamos um

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
`the-citrix-strategy-for-windows-7-virtual-desktop-users/>`).			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 “green bubbles”)	7.15 LTSR (e StoreFront 3.12)	1903	Experiência unificada do Citrix Receiver para Web.
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.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
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 compatível mais recente.
Studio no Windows 7, Windows 8 e Windows 8.1 (incluindo Service Packs)	7.15 LTSR	7.18	Instale o Studio em um sistema operacional compatível.
Redirecionamento de Flash	7.15 LTSR	1912	Crie conteúdo de vídeo como Vídeo HTML5. Use a Redireção de Vídeo HTML5 para conteúdo gerenciado e a Redireção de Conteúdo do Navegador para sites públicos. Para obter mais informações, consulte a nota Fim da Vida Útil da Redireção Flash.
Integração Citrix Online (produto Goto) com StoreFront	7.14 (e StoreFront 3.11)	StoreFront 3.12	
A conta de usuário, CtxAppVCOMAdmin,	7.14	7.14	O serviço do Windows

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
que foi criada durante a instalação do VDA e adicionada ao Grupo de Administradores Locais na máquina VDA, não é mais criada. O mecanismo "COM" subjacente também é removido.			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 para Web no Internet Explorer 8	7.13	7.13	
Opção de instalação de linha de comando do VDA /no_appv para evitar a instalação dos componentes 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	7.13	7.13	Alguns comandos PowerShell que eram fornecidos pelo snap-in Citrix.Common.Commands ainda estão

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
automaticamente ao atualizar instalações existentes.			disponíveis no SDK do XenApp 6.5.
Funcionalidade parcial para manipular dados de ícones que era fornecida pelos cmdlets *-CtxIcon.	7.13	7.13	Agora fornecido pelos cmdlets *-BrokerIcon 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.
Atualizações in-loco do StoreFront 2.0, 2.1, 2.5 e 2.5.2	7.13	7.16	Atualize de uma dessas versões para uma versão posterior compatível e depois para o XenApp e XenDesktop 7.16.
Atualizações 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 atualize para o XenDesktop 7.6 LTSR (com o CU

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

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
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 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 do sistema neste documento eram válidos quando esta versão do produto foi lançada. As atualizações são feitas periodicamente. Os requisitos do 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 de 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 servidores Windows, as instalações do Nano Server não são suportadas, salvo indicação em contrário. 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
License Server	8 GB de RAM; consulte a documentação de Licenciamento para recomendações de disco

Dimensionamento de VMs que fornecem desktops e aplicativos

Recomendações específicas não podem ser fornecidas devido à natureza complexa e dinâmica das ofertas de hardware, e cada implantação tem necessidades exclusivas. 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 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 primeiro passo. 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 2019, Edições Express, Standard e Enterprise.
- SQL Server 2017, Edições Express, Standard e Enterprise.
    - Para novas instalações: Por padrão, o SQL Server Express 2017 com Cumulative Update 16 é instalado ao instalar o Controller, se uma instalação existente e compatível do SQL Server não for detectada.
    - Para atualizações, nenhuma versão existente do SQL Server Express é atualizada.
- SQL Server 2016 SP2, Edições Express, Standard e Enterprise.

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

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

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

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

- Ao instalar um Controller, o Microsoft SQL Server Express LocalDB 2019 com a Atualização Cumulativa 20 é instalado para uso com o recurso Cache de Host Local. (Esta instalação é separada da instalação padrão do SQL Server Express para o banco de dados do site.)
- Ao atualizar um Controller, a versão existente do Microsoft SQL Server Express LocalDB não é atualizada automaticamente. Para 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 compatíveis mais atuais
- Orientação de dimensionamento de banco de dados
- Cache de Host Local

Citrix Studio

Sistemas operacionais compatíveis:

- Windows Server 2022
- Windows Server 2019, Edições Standard e Datacenter
- Windows Server 2016, Edições Standard e Datacenter
- Windows 11

- Windows 10 (somente 64 bits)

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Management Console 3.0 (incluído com todos os sistemas operacionais suportados).
- Windows PowerShell 3.0, 4.0 ou 5.0.

Citrix Director

Sistemas operacionais suportados:

- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter, e com a opção Server Core
- Windows Server 2016, edições Standard e Datacenter, e com a opção Server Core

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 inserir a mídia de instalação do Windows Server. Em seguida, esse software será instalado para você.
- Para visualizar os logs de eventos em máquinas onde o Citrix Director está instalado, você deve instalar o Microsoft .NET Framework 2.0.

Citrix Profile Management:

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

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

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Navegadores suportados para visualização do Director:

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

A resolução de tela ideal recomendada para visualização do Director é 1366 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 Acesso Remoto a PC usa este VDA, que você instala em PCs físicos de escritório. Este VDA oferece suporte a Secure Boot para Citrix Virtual Desktops™ Acesso Remoto a PC 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 multi-sessão

Sistemas operacionais suportados:

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

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 a instalação de um VDA em um sistema operacional Windows que não é mais compatível, consulte Sistemas operacionais anteriores.

Hosts / recursos de virtualização

Os seguintes recursos de host/virtualização (listados em ordem alfabética) são compatíveis. Onde aplicável, as versões *principal.secundária* são compatíveis, incluindo atualizações para essas versões. O artigo da Knowledge Center 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 Microsoft System Center Configuration Manager mínimo 2012.

Hipervisores suportados:

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

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

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

  Inclui qualquer versão do Hyper-V que possa se registrar com as versões compatíveis do System Center Virtual Machine Manager.

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

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

- **Nutanix Acropolis**

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

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

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

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

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

  Para obter mais informações, consulte VMware virtualization environments.

Hosts de nuvem pública suportados:

- **Amazon Web Services (AWS)**

  Para obter informações sobre como usar o AWS para provisionar máquinas virtuais, consulte a seção Ambientes de virtualização do Amazon Web Services da documentação do Citrix DaaS.

- **Google Cloud Platform**

  Para obter informações sobre como usar o Google Cloud para provisionar máquinas virtuais, consulte a seção Ambientes do Google Cloud da documentação do Citrix DaaS e o Guia de Implantação.

- **Microsoft Azure Resource Manager**

  Para obter informações sobre como usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais, consulte a seção Ambientes de virtualização do Microsoft Azure Resource Manager da documentação do Citrix DaaS.

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

- Você precisa de uma 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.
- 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 Configuração Completa. No Citrix Virtual Apps and Desktops™ local, a interface de gerenciamento é conhecida como Citrix Studio.
- As atualizações são lançadas para o Citrix DaaS aproximadamente a cada quatro semanas. Portanto, você pode descobrir que certos recursos disponíveis com o Citrix DaaS não estão disponíveis na versão local.

Níveis funcionais do Active Directory

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

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

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

HDX

Áudio

O áudio UDP para Multi-Stream ICA® é suportado no Citrix Workspace app para Windows e Citrix Workspace app para Linux 13.

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

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

Entrega de mídia do Windows HDX

Os seguintes clientes são suportados para busca de conteúdo do lado do cliente do Windows Media, redirecionamento do Windows Media e transcodificação multimídia 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):

- GPU Passthrough está disponível com:
  - Citrix 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:
  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere

Consulte `<https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html>`.

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 compactação baseada em CPU (incluindo compactação sem perdas), o HDX 3D Pro oferece suporte a qualquer adaptador de vídeo no computador host que seja compatível com o aplicativo que está sendo entregue.
- Para aceleração gráfica virtualizada usando a API NVIDIA GRID, você pode usar o HDX 3D Pro com todas as GPUs NVIDIA GRID compatíveis com o driver GRID 10 (consulte NVIDIA GRID). O NVIDIA GRID oferece uma alta taxa de quadros, resultando em uma experiência de usuário altamente interativa.
- A aceleração gráfica virtualizada é compatível com a plataforma gráfica de data center da família de processadores Intel Xeon E3. Para obter mais informações, consulte `<https://www.citrix.com/intel>` e `<https://www.intel.com/content/www/us/en/servers/data-center-graphics.html>`.
- A aceleração gráfica virtualizada é compatível com o AMD RapidFire em placas de servidor AMD FirePro série S. Consulte Solução de Virtualização AMD).

Dispositivo do usuário:

- O HDX 3D Pro oferece suporte a todas as resoluções de monitor compatíveis com a GPU no computador host. Para um desempenho ideal com as especificações mínimas recomendadas de dispositivo de usuário e GPU, a Citrix recomenda uma resolução máxima de monitor de 1920 x 1200 pixels para conexões LAN e 1280 x 1024 pixels para conexões WAN.
- A Citrix recomenda que os dispositivos do usuário tenham pelo menos 1 GB de RAM e uma CPU com uma velocidade de clock de 1,6 GHz ou superior. O uso do codec de compactação profunda padrão, que é necessário em conexões de baixa largura de banda, requer uma CPU mais potente, a menos que a decodificação seja feita em hardware. Para um desempenho ideal, a Citrix recomenda que os dispositivos do usuário tenham pelo menos 2 GB de RAM e uma CPU dual-core com uma velocidade de clock de 3 GHz ou superior.
- Para acesso a vários monitores, a Citrix recomenda dispositivos de usuário com CPUs quad-core.
- Os dispositivos do usuário não precisam de uma GPU para acessar desktops ou aplicativos entregues com o HDX 3D Pro.
- O aplicativo Citrix Workspace deve ser instalado.

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

Servidor de Impressão Universal

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

O componente UpsServer é suportado em:

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

Requisitos:

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

Para VDAs para SO de Múltiplas Sessões, a autenticação do usuário durante as operações de impressão exige 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 posterior são suportados. Para obter mais informações, consulte Licenciamento.

Ao usar o Citrix Provisioning (anteriormente Provisioning Services) com esta versão, a versão 7.x é coberta pelo ciclo de vida do XenApp e XenDesktop 7.x e pelo ciclo de vida do Citrix Virtual Apps and Desktops. 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 runtime 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 Citrix Workspace app para Windows não é instalado quando você instala um VDA atual. Para obter mais informações, consulte a documentação do Citrix Workspace app para Windows.

Consulte App-V para as versões suportadas do Microsoft App-V.

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

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

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

Visão geral técnica

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

Citrix Virtual Apps and Desktops permitem:

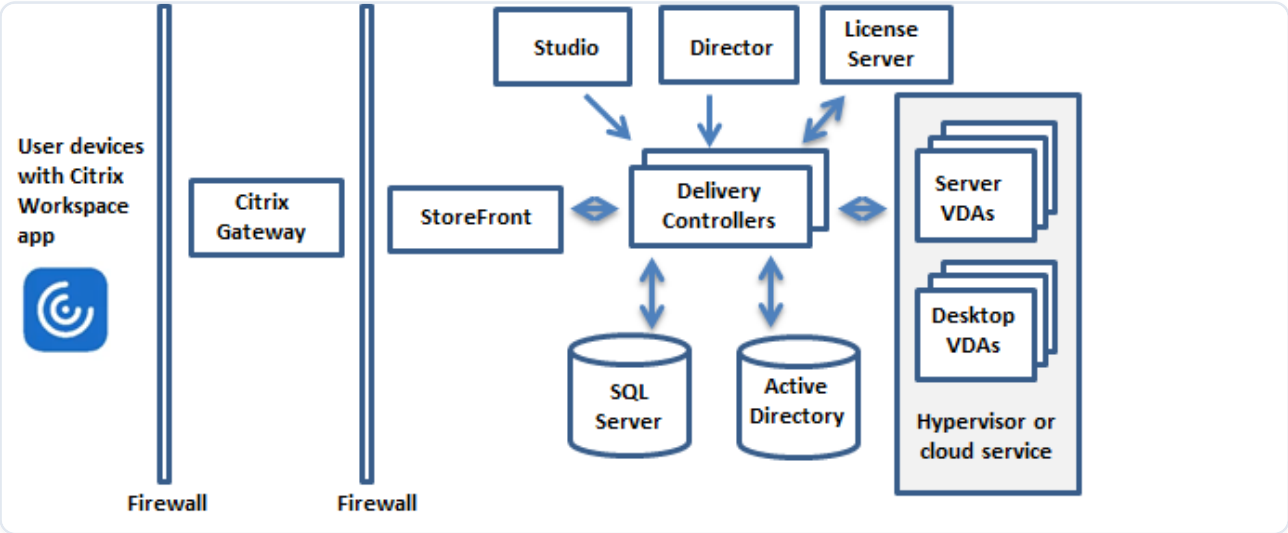
- Que os usuários finais executem aplicativos e desktops independentemente do sistema operacional e da interface do dispositivo.
- Que os administradores gerenciem a rede e controlem o acesso de dispositivos selecionados ou de todos os dispositivos.
- Que os administradores gerenciem uma rede inteira 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 central de gerenciamento de um site. Cada site tem 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 hipervisor 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 dessas 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. Em algumas edições, o Controller permite instalar o Profile Management para gerenciar as configurações de personalização do usuário em ambientes Windows virtualizados ou físicos.

Banco de dados

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

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

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 políticas configuradas para a sessão.

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

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

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

Citrix StoreFront™

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

Aplicativo Citrix Workspace™

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

Citrix Studio

O Studio é o console de gerenciamento onde você configura e gerencia sua implantação do Citrix Virtual Apps and Desktops. O Studio elimina a necessidade de consoles de gerenciamento separados para gerenciar a entrega de aplicativos e desktops. O Studio oferece 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 Studio obtém as informações que exibe do Serviço Broker no Controller, comunicando-se pela porta TCP 80.

Citrix Director

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

O Director exibe:

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

Citrix License Server

O License Server gerencia suas licenças de produtos Citrix. Ele se comunica com o Controller para gerenciar o licenciamento para a sessão de cada 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 hipervisores e outros serviços.

Embora muitas implantações exijam um hypervisor, você não precisa de um para fornecer Acesso Remoto ao 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 provisionamento de 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 hipervisor 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

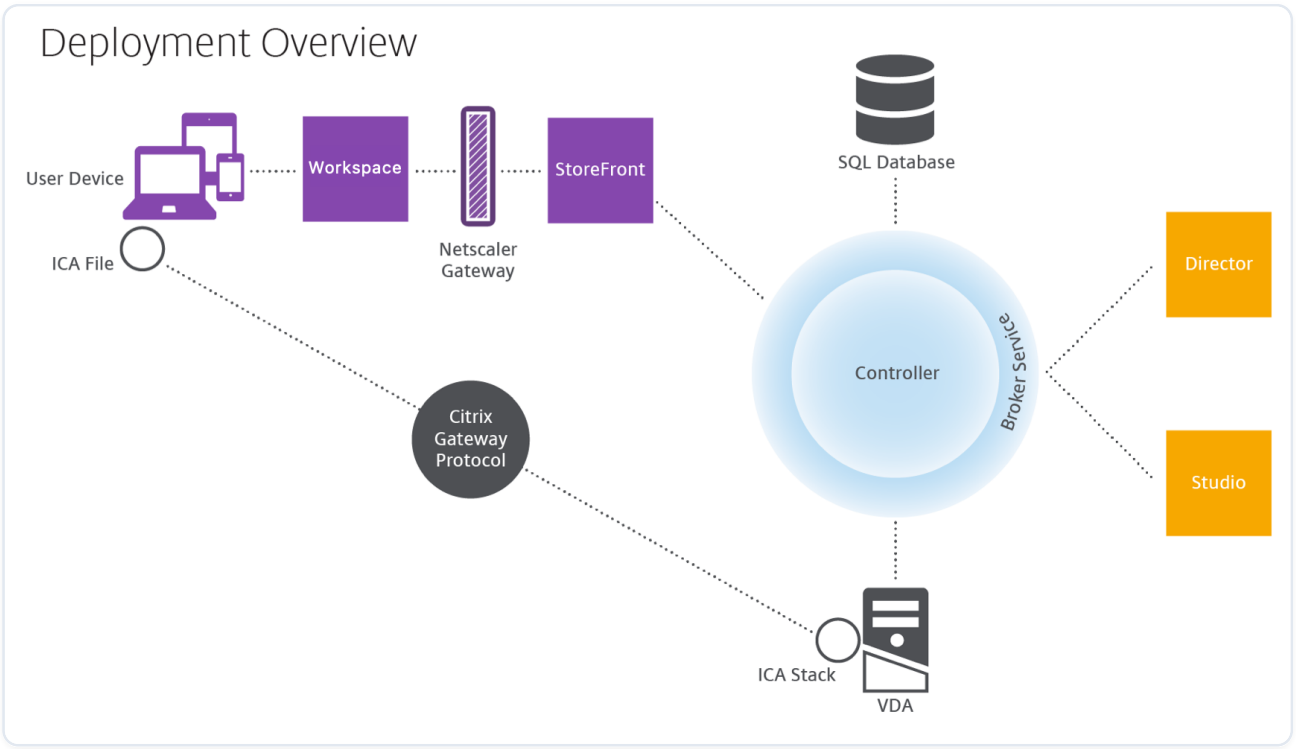
Quando os usuários se conectam de fora do firewall corporativo, o Citrix Virtual Apps and Desktops pode usar a tecnologia Citrix Gateway (anteriormente Access Gateway e NetScaler® Gateway) para proteger essas conexões com TLS. O Citrix Gateway ou o appliance virtual VPX é um appliance SSL VPN que é implantado 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 compactação 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.



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 tem 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.

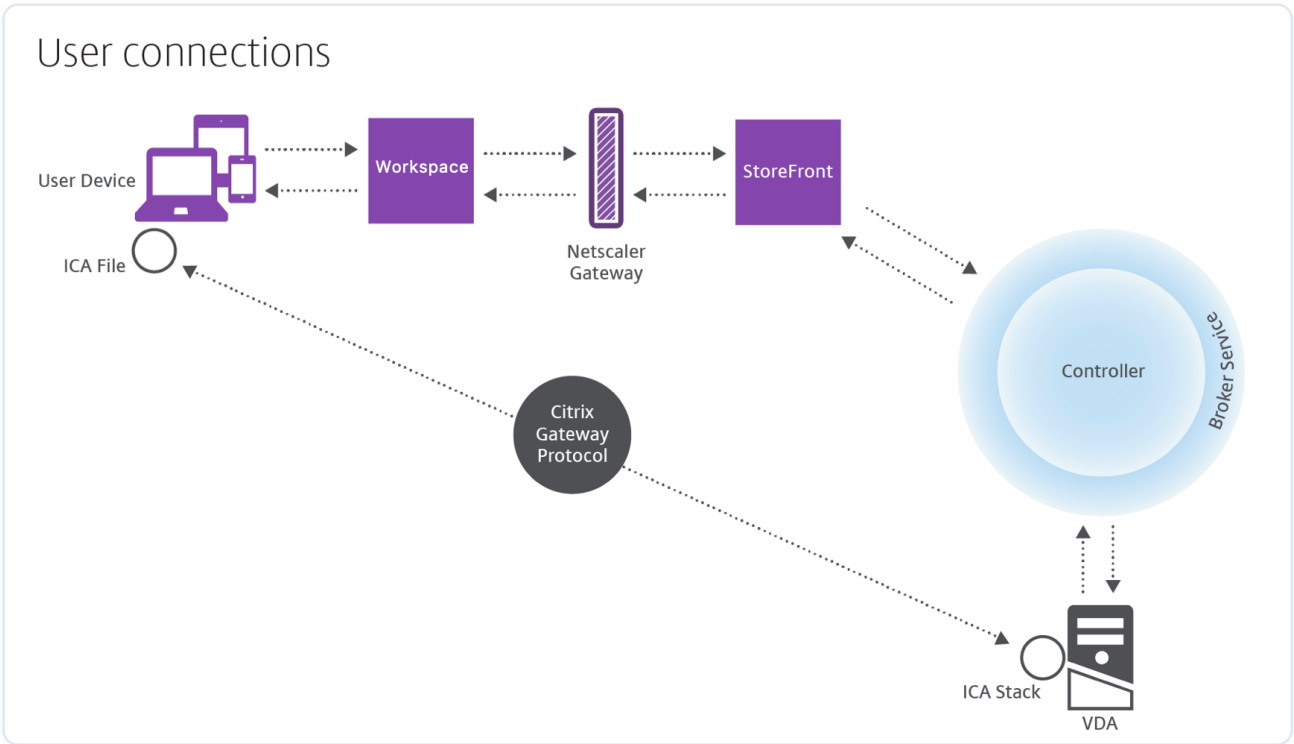
Os usuários nunca acessam diretamente o Controller. O VDA serve como um intermediário entre os usuários e o Controller. Quando os usuários fazem logon usando o StoreFront, suas credenciais são passadas para o Broker Service no Controller. O Broker Service então obtém perfis e recursos disponíveis com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

Como as conexões do 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 do StoreFront.

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

As credenciais do usuário se movem por esse 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.



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

Após a verificação das credenciais, as informações sobre os aplicativos ou desktops disponíveis são enviadas de volta ao usuário através do caminho StoreFront-aplicativo Citrix Workspace.

Quando o usuário seleciona aplicativos ou desktops desta lista, essa informação retorna pelo caminho até o Controller. O Controller então determina o VDA apropriado para hospedar os aplicativos ou desktop específicos.

O Controller envia uma mensagem ao VDA com as credenciais do usuário e, em seguida, envia todos os dados sobre o usuário e a conexão para o VDA. O VDA aceita a conexão e envia as informações de volta pelos mesmos caminhos para o aplicativo Citrix Workspace. Um conjunto de parâmetros necessários é coletado no StoreFront. Esses parâmetros são então enviados para o 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 esse processo.

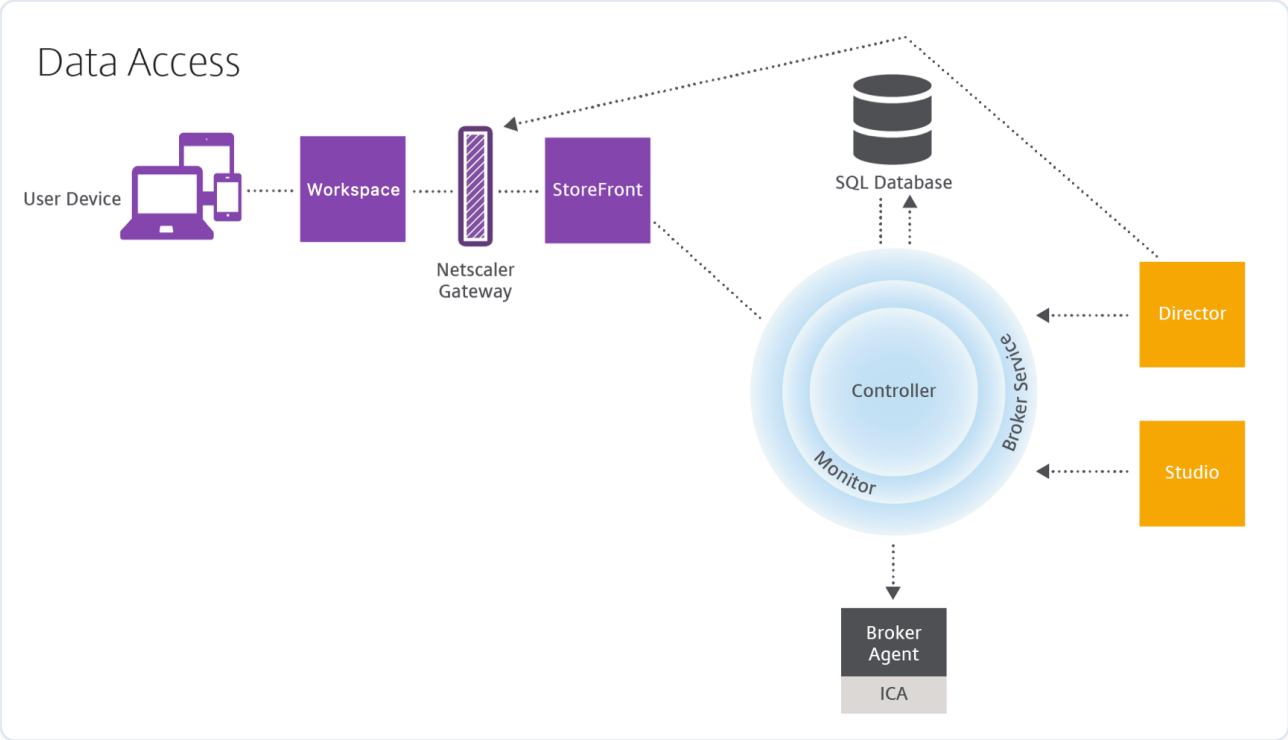
O arquivo ICA é copiado para o dispositivo do usuário e estabelece uma conexão direta entre o dispositivo e a pilha ICA em execução no VDA. Essa conexão ignora a infraestrutura de gerenciamento (aplicativo Citrix Workspace, StoreFront e Controller).

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

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

Entregar desktops e aplicativos

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

Catálogos de máquinas

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

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

Os tipos de máquina válidos são:

- **SO multi-sessão:** Máquinas virtuais ou físicas com um sistema operacional multi-sessão. 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 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 seu grupo do Active Directory, porque os grupos do Active Directory e os grupos de entrega são maneiras de agrupar usuários com requisitos semelhantes.

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

Você define quais recursos os usuários no grupo de entrega podem acessar. Por exemplo, para entregar aplicativos diferentes a usuários diferentes, 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 mais informações, consulte Criar grupos de entrega.

Grupos de aplicativos

Grupos de aplicativos fornecem vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega. Usando o recurso de restrição de tags, 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 considerada 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 mais informações, consulte Criar grupos de aplicativos.

Mais informações

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

Active Directory

O Active Directory é necessário para autenticação e autorização. A infraestrutura Kerberos no Active Directory é usada para garantir a autenticidade e confidencialidade das comunicações com os Delivery Controllers. Para obter informações sobre 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 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 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 floresta do Active Directory múltipla

Esta informação se aplica à versão mínima XenDesktop 7.1 e XenApp 7.5. Não se aplica a versões anteriores do XenDesktop ou XenApp.

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 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 de registro ao VDA e aos Delivery Controllers:

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

> No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Em todos os Delivery Controllers, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Você pode precisar de configuração de DNS reverso se o seu namespace DNS for diferente do do Active Directory.

Uma entrada de registro foi adicionada para evitar a habilitação indesejada da autenticação NTLM em VDAs, que é menos segura que o Kerberos. Esta entrada pode ser usada em vez da entrada `SupportMultipleForest`, que ainda pode ser usada para compatibilidade com versões anteriores.

No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`.

- Nome: `SupportMultipleForestDdcLookup`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Esta chave de registro executa uma pesquisa DDC em um ambiente de floresta múltipla 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 Controlador de Domínio 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
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.

Bancos de dados

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.
- **Registro de configuração:** (também conhecido como registro) armazena informações sobre alterações na configuração do site e atividades administrativas. Este banco de dados é usado quando o recurso de registro 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 funcionando até que um usuário faça logoff ou se desconecte. Para obter informações sobre o comportamento da conexão quando o banco de dados do site se torna indisponível, consulte Cache de Host Local.

A Citrix recomenda que você faça backup dos bancos de dados regularmente para que 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 instruções, consulte CTX135207.

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 de Cluster de Failover do Windows Server (WSFC). Para obter mais informações, consulte Clustering de Failover do Windows Server com SQL Server.
- **Espelhamento de banco de dados do 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 ocorrerá 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 esta solução é mais complicado, e o processo de failover automático é tipicamente mais lento do que alternativas como o espelhamento SQL.
- **Uso dos recursos de alta disponibilidade do hipervisor:** Com este método, você implanta o banco de dados como uma máquina virtual e usa os recursos de alta disponibilidade do seu hipervisor. Esta solução é menos cara do que o espelhamento porque usa 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 Cache de Host Local complementa as melhores práticas de alta disponibilidade do SQL Server. O Cache de Host Local 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 Cache de Host Local.

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.

Não há suporte para a instalação de um Controller em um nó em uma instalação de cluster SQL ou espelhamento SQL.

Instalar software de banco de dados

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

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

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

Para a maioria das implantações de produção e qualquer implantação que use recursos de alta disponibilidade da Microsoft, recomendamos usar apenas edições não Express suportadas do SQL Server. Instale o SQL Server em máquinas diferentes do servidor onde o primeiro Controller

está instalado. Requisitos do sistema lista as versões suportadas do SQL Server. Os bancos de dados podem residir em uma ou mais máquinas.

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

Use o Windows Update para manter o SQL Server atualizado.

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

Especifique os nomes e endereços (localização) do banco de dados na página **Bancos de Dados** no assistente de criação de site. (Consulte Formatos de endereço de banco de dados.) Para evitar possíveis erros quando o Director consultar 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 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 log de configuração e do banco de dados de monitoramento posteriormente, depois de criar o site. Consulte Alterar locais de 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 que será 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 em um endereço especificado, ele deverá 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 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. A sequência é a seguinte:

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

   Você pode indicar onde armazenar os scripts.

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

> scripts, você também pode usar o PowerShell. Para obter detalhes, consulte Preferred database rights scripts.

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

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

- Use 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 SQL Server Read-Committed Snapshot. 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 do SQLCMD.

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

O Studio solicita que você continue a criação do site. Você é retornado à página **Bancos de Dados**. Insira os endereços. Se algum dos servidores que hospedam 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 seguintes permissões podem ser explicitamente configuradas ou adquiridas por meio da associação a grupos do Active Directory. Se suas credenciais de usuário do Studio não incluírem essas permissões, você será solicitado a fornecer as credenciais de usuário do SQL Server.

OPERAÇÃO	PROPÓSITO	FUNÇÃO DO SERVIDOR	FUNÇÃO DO BANCO DE DADOS
Criar um banco de dados	Criar um banco de dados vazio adequado	`dbcreator`	
Criar um esquema	Criar todos os esquemas específicos do serviço e adicionar o primeiro Controller ao site	`securityadmin` *	`db_owner`
Adicionar um Controller	Adicionar um Controller (diferente do primeiro) ao site	`securityadmin` *	`db_owner`
Adicionar um Controller (servidor espelho)	Adicionar um login de Controller ao servidor de banco de dados atualmente na função de espelho de um banco de dados espelhado	`securityadmin` *	
Remover Controller	Remover controlador do site	**	`db_owner`
Atualizar um esquema	Aplicar atualizações de esquema ou hotfixes		`db_owner`

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

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

Ao usar o Studio para realizar essas operações, o usuário do 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 logon 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 de banco de dados. Essas tarefas exigem direitos `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 uma das seguintes formas:

- `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 servidor SQL autônomo, o Espelhamento de Banco de Dados e a Alta Disponibilidade AlwaysOn, consulte este artigo CTX.

Alterar locais de 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 habilitado.

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. Selecione **Configuração** no painel de navegação do Studio.
3. Selecione o banco de dados para o qual você deseja especificar um novo local e, em seguida, selecione **Alterar Banco de Dados** no painel **Ações**.
4. Especifique o novo local e o nome do banco de dados.
5. Se você deseja que o Studio crie o banco de dados e tiver as permissões apropriadas, clique em **OK**. Quando solicitado, clique em **OK**, e então o Studio o cria automaticamente. O 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 Studio então carrega o esquema

do banco de dados para o mesmo. As credenciais são retidas apenas durante o período de criação do banco de dados.

6. Se você não deseja que o Studio crie o banco de dados, ou se você não tem permissões suficientes, clique em **Gerar script**. 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 aos desktops 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 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 Citrix Provisioning) e muitas camadas de aplicativos, 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 executada 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 multiusuário para entregar aplicativos publicados e desktops publicados 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 fornecido por você.
- Os aplicativos são entregues virtualmente e exibidos perfeitamente em alta definição nos dispositivos do usuário.
- Dependendo das configurações de perfil, as alterações do usuário são salvas quando a sessão do aplicativo do usuário termina. Caso contrário, as alterações são excluídas.

Processar, hospedar e entregar aplicativos:

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

Gerenciamento e atribuição de sessão:

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

  Por exemplo, um usuário faz logon e solicita um aplicativo. Uma sessão nessa máquina fica indisponível para outros usuários. Um segundo usuário faz logon e solicita um aplicativo que essa máquina hospeda. Uma segunda sessão na mesma máquina agora está indisponível. Se ambos os usuários solicitarem mais aplicativos, nenhuma sessão adicional será necessária porque um usuário pode executar vários aplicativos usando a mesma sessão. Se mais dois usuários fizerem logon e solicitarem desktops, e duas sessões estiverem disponíveis nessa 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 que está configurado para hospedar o mesmo aplicativo. Você também pode atribuir estaticamente uma única máquina para entregar um aplicativo a um único usuário cada vez que esse usuário fizer logon. Máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de múltiplas sessões não é suportada em máquinas de SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega ao fazer logon, e os usuários devem estar online para acessar seus aplicativos.
- Este método pode aumentar a quantidade de recursos do servidor para processamento de aplicativos e aumentar a quantidade de armazenamento para os 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.

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

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

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

- **Desktop não persistente aleatório, também conhecido como desktop VDI agrupado:** Cada vez que um usuário faz logon em um desses desktops, esse usuário se conecta a um desktop selecionado de um pool de desktops. Esse pool é baseado em uma única imagem mestre. Todas as alterações no desktop são perdidas quando a máquina é reiniciada.
- **Desktop não persistente estático:** 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 persistente estático:** 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 Remote PC Access 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 Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, desktops virtuais ou aplicativos e sua infraestrutura associada.

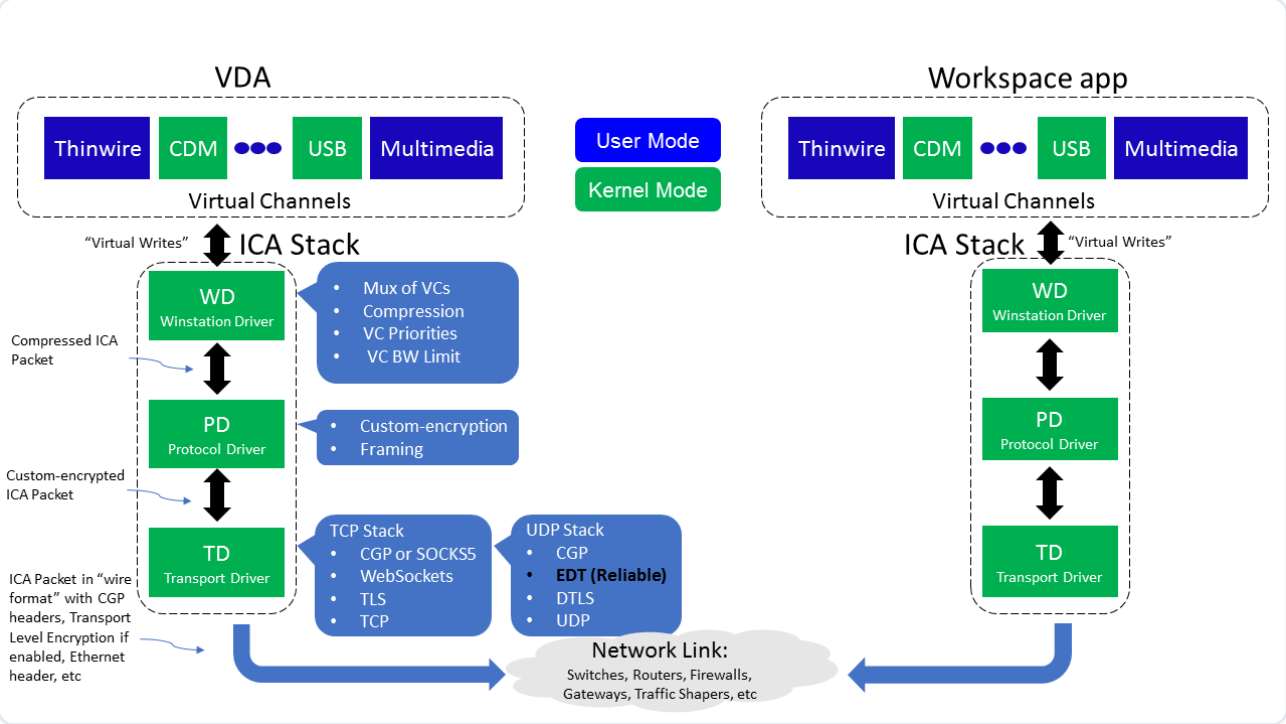
O Remote PC Access usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam desktops e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos exigidos para a implantação do Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários recebem a melhor experiência do usuário usando o Citrix HDX™ para entregar sua sessão de PC do escritório.

Para obter mais informações, Remote PC Access.

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 aos usuários de aplicativos e desktops centralizados, em qualquer dispositivo e em qualquer rede.

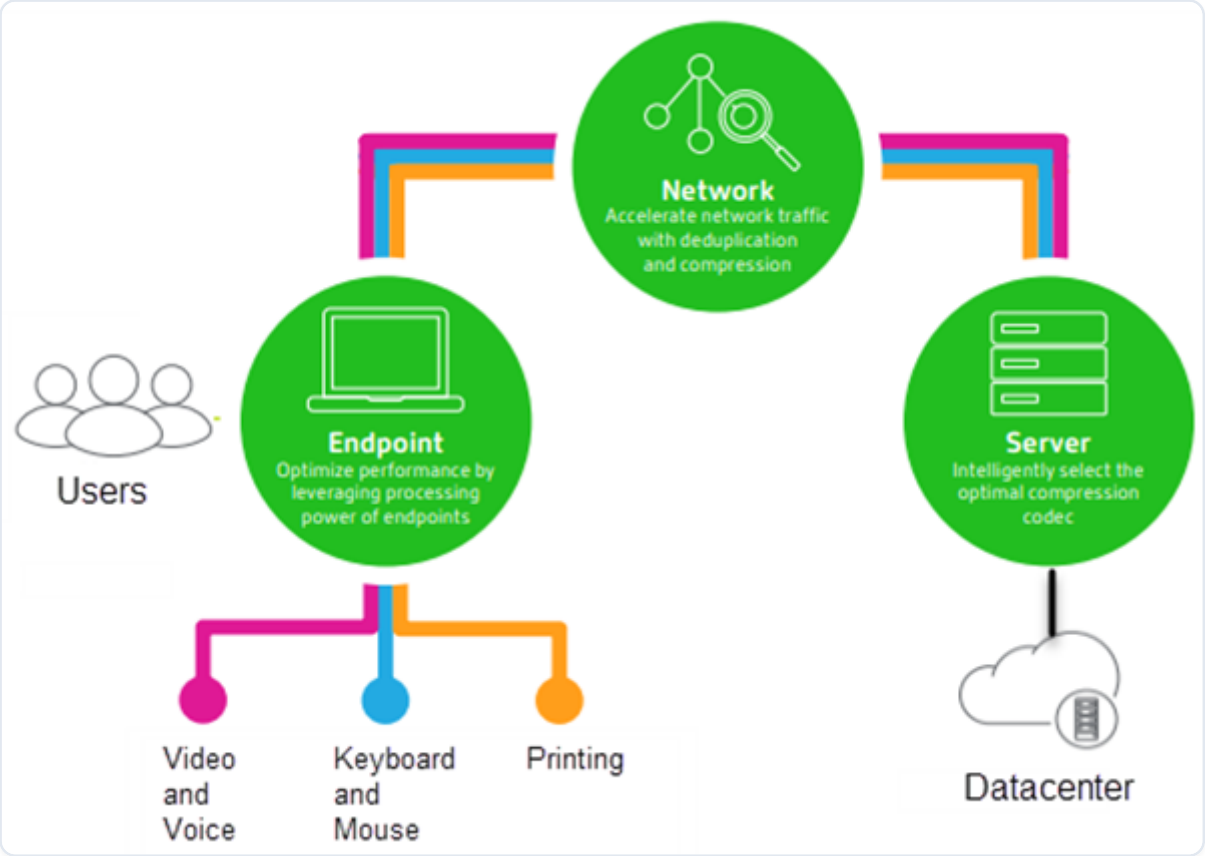


O HDX é projetado com base em três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

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

- **Redirecionamento inteligente** - O redirecionamento inteligente examina a atividade da tela, comandos de aplicativos, dispositivo de endpoint e 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 os dados agregados enviados entre cliente e servidor. Isso é feito aproveitando padrões repetidos em dados comumente acessados, como gráficos bitmap, documentos, trabalhos de impressão e mídia transmitida. O cache desses padrões permite que apenas as alterações sejam transmitidas pela rede, eliminando o tráfego duplicado. O HDX também suporta a transmissão multicast de fluxos multimídia, onde uma única transmissão da fonte é visualizada por vários assinantes em um local, em vez de uma conexão um-para-um para cada usuário.

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

No dispositivo

O HDX usa a capacidade de computação dos dispositivos do usuário para aprimorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários recebam uma experiência suave e contínua com conteúdo multimídia em seus desktops ou aplicativos virtuais. O controle de espaço de trabalho permite que os usuários pausem desktops e aplicativos virtuais e retomem o trabalho de um dispositivo diferente no ponto em que pararam.

Na rede

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

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

No data center

O HDX 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 (round-trip time) do ICA de cada sessão.

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

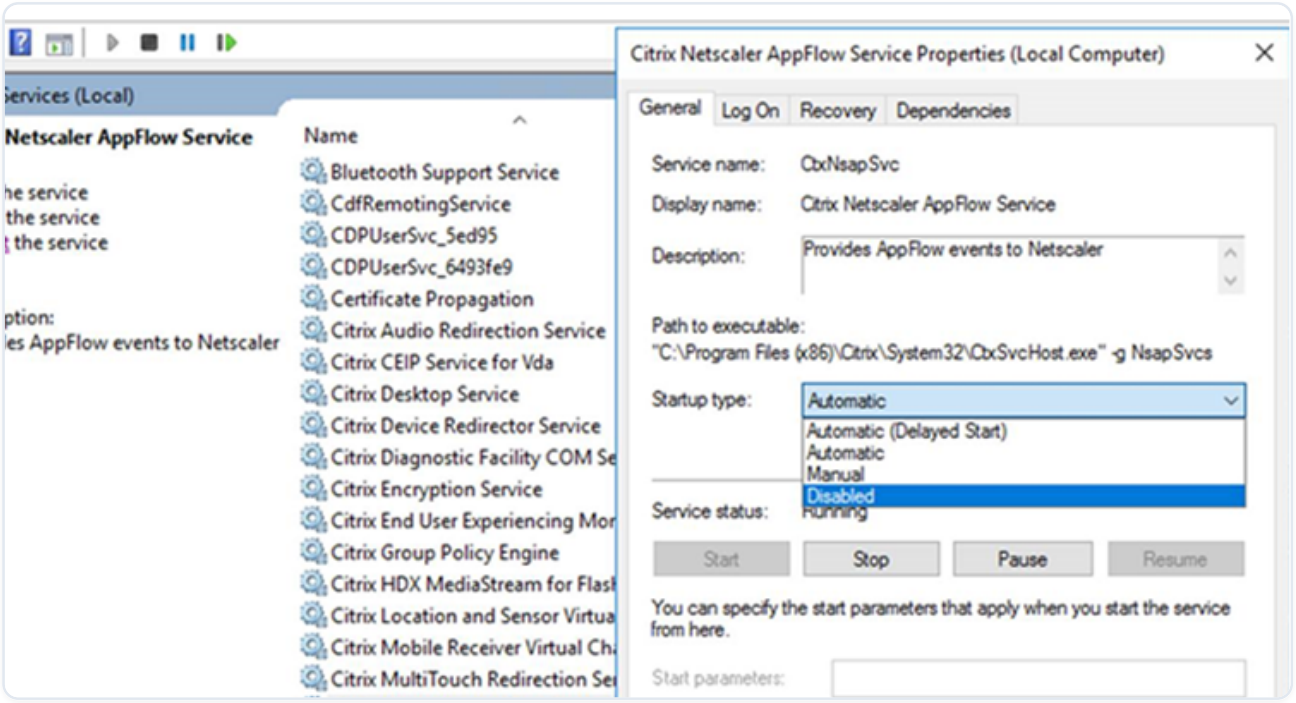
Requisitos mínimos:

- Citrix Virtual Apps e Desktops™ 7 v1808
- XenApp e XenDesktop 7.17
- NetScaler versão 12.0 Build 57.x
- Citrix Workspace™ app para Windows 1808
- Citrix Receiver para Windows 4.10

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

Habilitar ou desabilitar o canal virtual 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.

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

- O HDX seleciona automaticamente o melhor método de entrega com base no cliente, plataforma, aplicativo e largura de banda da rede, e então se autoajusta com base nas condições variáveis.
- O HDX otimiza o desempenho de gráficos e vídeo 2D e 3D.
- O HDX permite que dispositivos de 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: visualize um vídeo em um site que contenha vídeos de alta definição, como `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`.

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 suportadas, além de desktops de Acesso Remoto a PC.
- Este conteúdo descreve como otimizar a experiência do usuário, melhorar a escalabilidade do servidor ou reduzir os requisitos de largura de banda. Para obter informações sobre como usar políticas e configurações de política do Citrix, consulte a documentação Políticas do Citrix para esta versão.

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

Reconexão automática do cliente e confiabilidade da sessão

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

Reconexão automática do cliente:

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

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

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

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

Configurações padrão de reconexão automática do cliente:

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

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

Confiabilidade da sessão:

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

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

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

Na reconexão, o cliente e o servidor retomam no mesmo ponto em que estavam em sua troca de protocolo. As janelas da sessão perdem a translucidez e pop-ups apropriados da área de notificação são mostrados 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: Ativado
- Número da porta de confiabilidade da sessão: 2598

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

NetScaler com reconexão automática do cliente e confiabilidade da sessão:

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

- A confiabilidade da sessão está desabilitada no NetScaler Gateway.

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

Taxa de transferência adaptativa HDX

A taxa de transferência adaptativa HDX ajusta inteligentemente a taxa de transferência máxima da sessão ICA, ajustando os buffers de saída. O número de buffers de saída é inicialmente definido com um valor alto. Esse valor alto permite que os dados sejam transmitidos ao cliente de forma mais rápida e eficiente, especialmente em redes de 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:

- Versão 1811 ou posterior do VDA
- Workspace app para Windows 1811 ou posterior

Melhorar a qualidade da imagem enviada para os dispositivos do usuário

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

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

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

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

Melhorar o desempenho da videoconferência

Vários aplicativos populares de videoconferência são otimizados para entrega a partir do Citrix Virtual Apps and Desktops por meio de redirecionamento multimídia (consulte, por exemplo, HDX RealTime Optimization Pack). Para aplicativos que não são otimizados, a compressão de vídeo da webcam HDX melhora a eficiência da largura de banda e a tolerância à latência para webcams durante 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 compressão de vídeo da webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em Configurações de política ICA > Configurações de política de dispositivos USB.

A compactação de vídeo de 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
- Redirecionamento de Mídia do Windows

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

Prioridades de tráfego de rede

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

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

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

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

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

> **Aviso:**
>
> Use segurança de transporte ao usar este recurso. A Citrix recomenda usar o Internet Protocol Security (IPsec) ou o Transport Layer Security (TLS). As conexões TLS são suportadas apenas quando as conexões atravessam um NetScaler Gateway que suporta ICA multi-stream. Em uma rede corporativa interna, conexões multi-stream com TLS não são suportadas.

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

- Política Multi-Porta - Esta configuração especifica portas para o tráfego ICA em múltiplas conexões e estabelece prioridades de rede.

  - Selecione uma prioridade na lista de prioridades de porta padrão do CGP. Por padrão, a porta primária (2598) tem prioridade Alta.
  - Digite mais portas CGP em CGP port1, CGP port2 e CGP port3 conforme necessário, e identifique as prioridades para cada uma. Cada porta deve ter uma prioridade única.

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

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

Mostrar ou ocultar a barra de idiomas remota

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

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

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

Mapeamento de teclado Unicode

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

Habilitar ou desabilitar o mapeamento de layout de teclado Unicode

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

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

Habilitar modo compatível de mapeamento de layout de teclado Unicode

Por padrão, o mapeamento de layout de teclado Unicode conecta automaticamente 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 oferecer suporte a essas aplicações não conectadas. Adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valor: 1

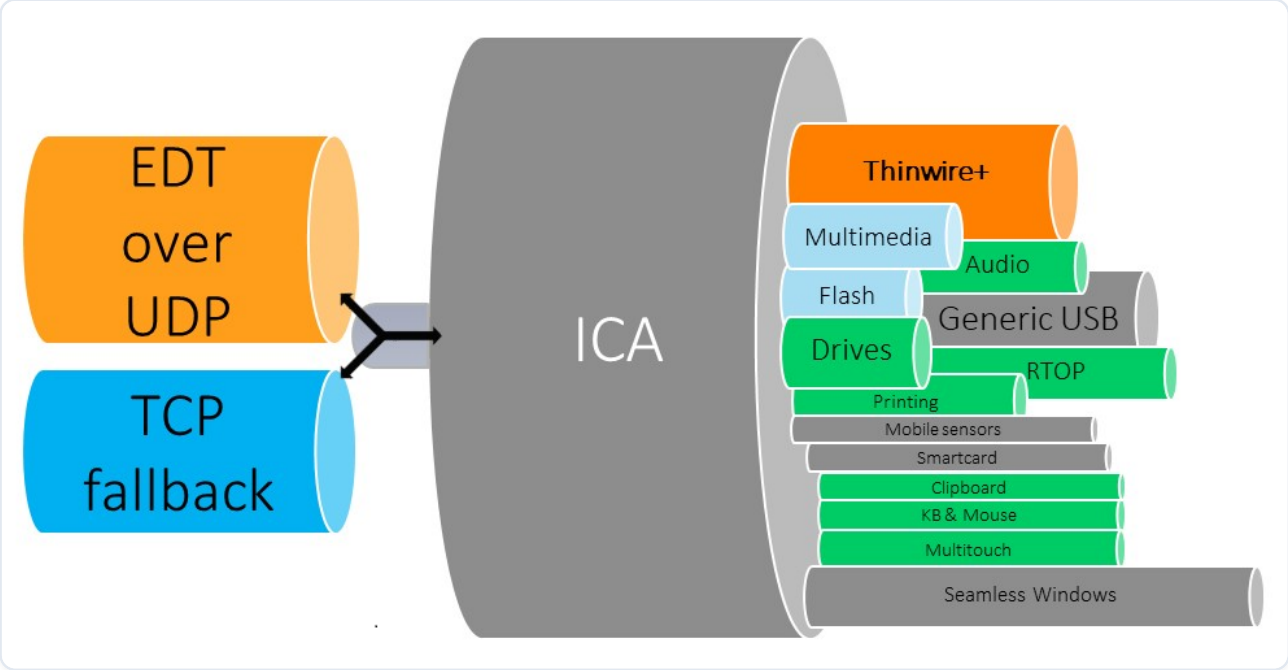
Para usar o mapeamento normal de layout de teclado Unicode, defina **DisableWindowHook** como 0.

Transporte adaptável

O Transporte Adaptável é um mecanismo no Citrix Virtual Apps and Desktops™ que oferece a capacidade de usar o Enlightened Data Transport (EDT) como protocolo de transporte para conexões ICA. O Transporte Adaptável muda para TCP quando o EDT não está disponível.

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

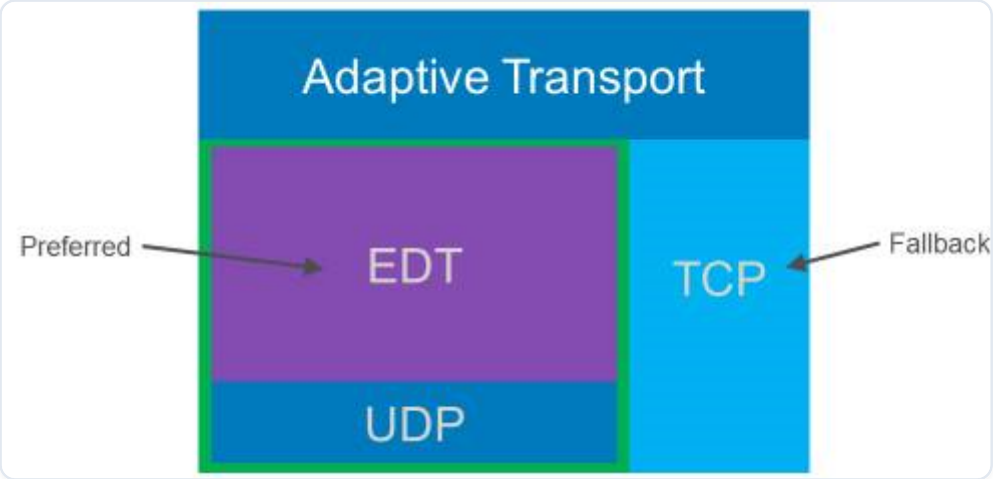
todos os canais virtuais ICA® em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.



Quando o Transporte Adaptável é definido como **Preferencial**, o EDT é usado como protocolo de transporte principal e o TCP é usado para fallback. Por padrão, o Transporte Adaptável é definido como **Preferencial**. Você pode definir o Transporte Adaptável para o **modo de diagnóstico** para fins de teste, o que permite apenas o EDT e desativa o fallback para TCP.

Com o aplicativo Citrix Workspace™ para Windows, Mac e iOS, as conexões EDT e TCP são tentadas em paralelo durante a conexão inicial, reconexão de confiabilidade da sessão e reconexão automática do cliente. Isso reduz o tempo de conexão se o transporte UDP subjacente estiver indisponível e o TCP precisar ser usado em vez disso. Se o Transporte Adaptável for definido como **Preferencial** e a conexão for estabelecida usando TCP, o Transporte Adaptável continua a tentar mudar para EDT a cada cinco minutos.

Com o aplicativo Citrix Workspace para Linux e Android, as conexões EDT são tentadas primeiro. Se a conexão não for bem-sucedida, o aplicativo Citrix Workspace tenta se conectar usando TCP após o tempo limite da solicitação EDT.



Requisitos do sistema

A seguir estão os requisitos para usar o Transporte Adaptável e o EDT:

- Plano de controle
  - Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops)
  - Citrix Virtual Apps and Desktops 1912 ou posterior
- Agente de Entrega Virtual
  - Versão 1912 ou posterior (2103 ou posterior recomendado)
  - A versão 2012 é o mínimo exigido para usar o EDT com o Citrix Gateway Service
- StoreFront™
  - Versão 3.12.x
  - Versão 1912.0.x
- Aplicativo Citrix Workspace
  - Windows: versão 1912 ou posterior (2105 ou posterior recomendado)
  - Linux: versão 1912 ou posterior (2109 ou posterior recomendado)
  - Mac: versão 1912 ou posterior (2108 ou posterior recomendado)
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível no Google Play
- Citrix Gateway (ADC)
  - 13.0.52.24 ou posterior

  - 12.1.56.22 ou posterior

- Firewall (da perspectiva do VDA)
  - UDP 1494 de entrada – se a confiabilidade da sessão estiver desabilitada
  - UDP 2598 de entrada – se a confiabilidade da sessão estiver habilitada
  - UDP 443 de entrada – se o SSL do VDA estiver habilitado para criptografia ICA (DTLS)
  - UDP 443 de saída – se estiver usando o Citrix Gateway Service. Para obter mais informações, consulte a documentação do Citrix Gateway service.

Considerações

- Habilite a confiabilidade da sessão para usar a Descoberta de MTU EDT e para usar o EDT com o Citrix Gateway e o Citrix Gateway service.
- Certifique-se de que o MTU do EDT esteja definido adequadamente para evitar a fragmentação. Caso contrário, o desempenho pode ser afetado ou as sessões podem falhar ao iniciar em algumas situações. Para obter mais informações, consulte a seção Descoberta de MTU do EDT.
- Para obter detalhes sobre os requisitos e considerações para usar o EDT com o serviço Citrix Gateway, consulte Transporte Adaptativo HDX com suporte EDT para o serviço Citrix Gateway.
- Para obter detalhes sobre a configuração do Citrix Gateway para oferecer suporte ao EDT, consulte Configurar o Citrix Gateway para oferecer suporte ao Enlightened Data Transport e HDX Insight.
- O IPv6 não é suportado atualmente.

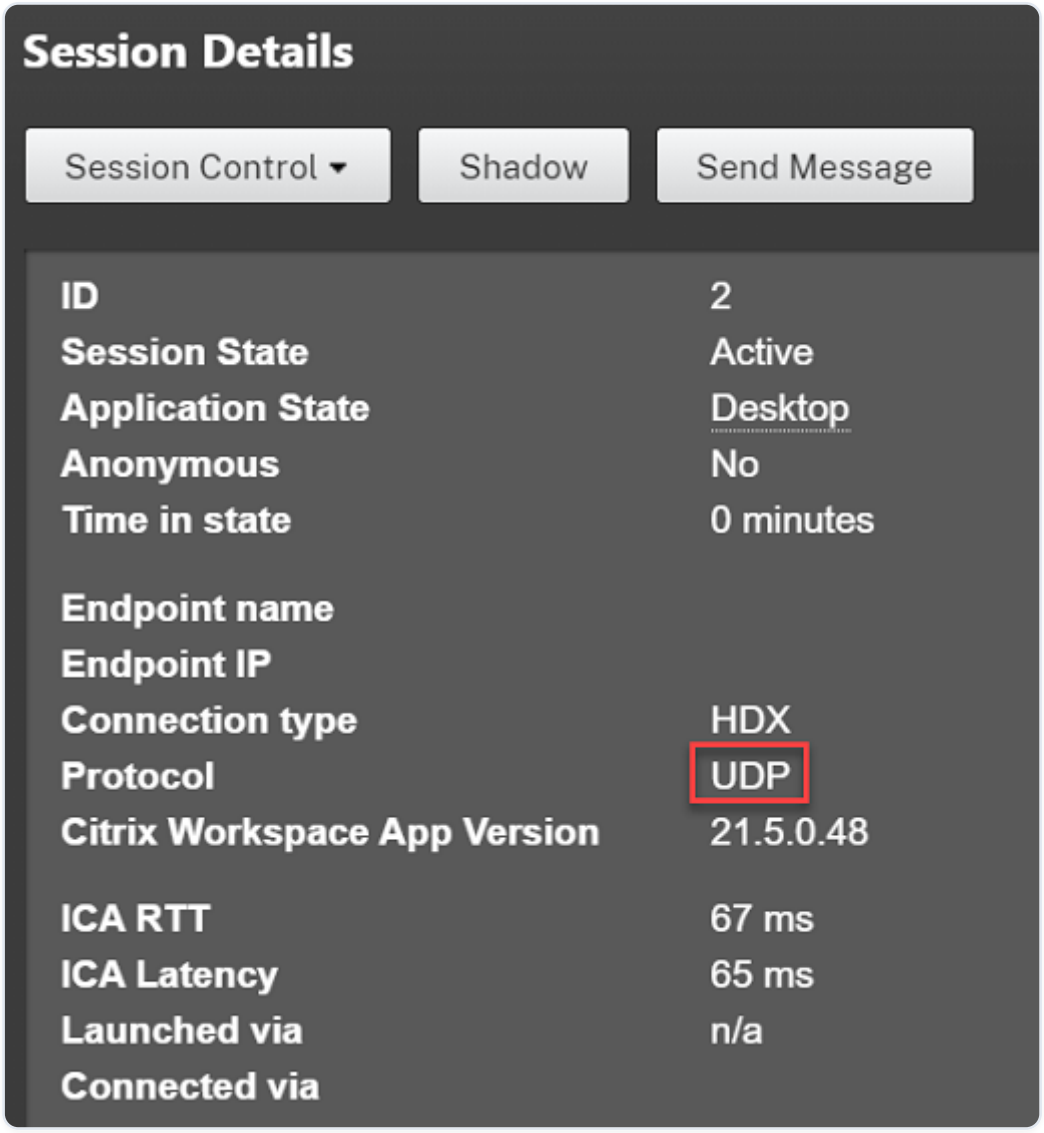
Configuração

O Transporte Adaptativo é habilitado por padrão. Você pode configurar as seguintes opções usando a configuração **HDX™ Adaptive Transport** na política do Citrix.

- **Preferencial**. Esta é a configuração padrão. O Transporte Adaptativo é habilitado e usa o EDT como protocolo de transporte preferencial, com fallback para TCP.
- **Modo de diagnóstico**. O Transporte Adaptativo é habilitado e força o uso do EDT. O fallback para TCP é desabilitado. Esta configuração é recomendada apenas para testes e solução de problemas.
- **Desativado**. O Transporte Adaptativo é desabilitado e apenas o TCP é usado para transporte.

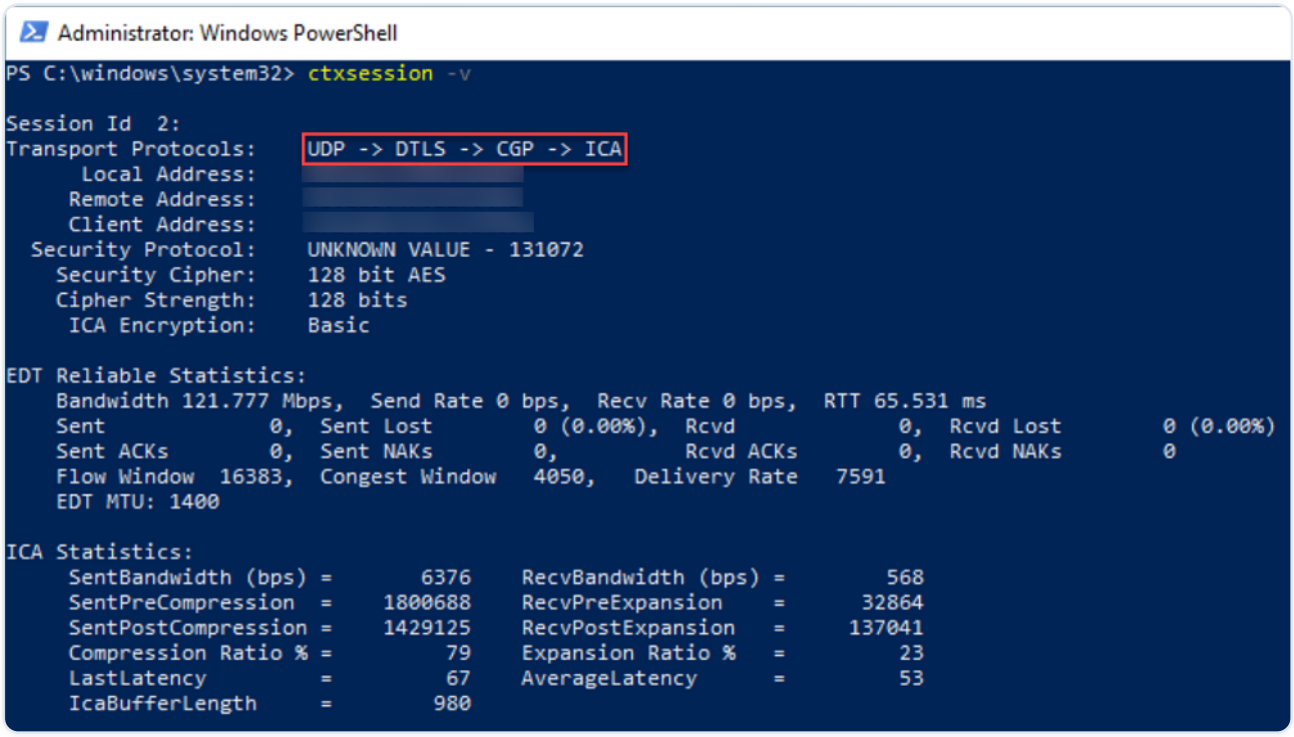
Para confirmar que o EDT está sendo usado como protocolo de transporte para a sessão, você pode usar o Director ou o utilitário de linha de comando CtxSession.exe no VDA.

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. Se o **Tipo de conexão** for **RDP**, o ICA não está em uso e o **Protocolo** exibe N/A. Para obter mais informações, consulte Monitorar sessões.



Para usar o utilitário CtxSession.exe, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe`. Para ver estatísticas detalhadas, execute `ctxsession.exe -v`. Se 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 com DTLS de ponta a ponta)



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.

Requisitos do sistema

- VDA versão mínima 1912 (2103 ou posterior recomendado)
- Aplicativo Citrix Workspace
  - Windows: versão 1912 ou posterior (2105 ou posterior recomendado)
  - Mac: versão 2108 ou posterior
  - Linux: versão 2109 ou posterior
  - Android: versão 21.5 ou posterior
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- A Confiabilidade da Sessão deve estar habilitada

Se você usa plataformas ou versões de cliente que não suportam esse recurso, consulte CTX231821 para obter detalhes sobre como configurar um MTU EDT personalizado que seja apropriado para seu ambiente.

Importante:

A Descoberta de MTU não é suportada com ICA Multi-Stream.

Para controlar a Descoberta de MTU EDT no VDA

A Descoberta de MTU está habilitada por padrão. Para desabilitar esse recurso, exclua o valor de registro **EDT MTU Discovery** e reinicie o VDA. Para obter mais informações, consulte a configuração EDT MTU Discovery na lista de recursos HDX gerenciados por meio do registro.

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.

Modo tolerante a perdas

Importante:

- O recurso requer no mínimo o aplicativo Citrix Workspace 2002 para Windows.
- O modo tolerante a perdas não é suportado no Citrix Gateway ou no Citrix Gateway Service. Este modo está disponível apenas com conexões diretas.

O modo tolerante a perdas usa o protocolo de transporte EDT Lossy para aprimorar a experiência do usuário para usuários que se conectam por meio de redes com alta latência e perda de pacotes.

Inicialmente, as sessões são estabelecidas usando EDT. Se os limites de latência e perda de pacotes forem atingidos ou excedidos, os canais virtuais aplicáveis mudam de EDT para EDT Lossy, enquanto os outros canais virtuais permanecem em EDT. Se a latência e a perda de pacotes diminuírem abaixo dos limites, os canais virtuais aplicáveis voltam para EDT.

Os limites padrão são:

- Perda de pacotes: 5%
- Latência: 300 ms (RTT)

O modo tolerante a perdas é ativado por padrão. Você pode desativar o modo ou ajustar os limites de perda de pacotes e latência usando a configuração de limites do modo tolerante a perdas.

Requisitos do sistema

- Citrix Virtual Delivery Agent (VDA) 2003
- Citrix Workspace app 2002 para Windows
- Confiabilidade da sessão ativada. Para obter mais informações sobre a confiabilidade da sessão, consulte Configurações de política de confiabilidade da sessão.

Problemas conhecidos

O Adaptive Transport e o EDT contêm os seguintes problemas:

- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha no lançamento de sessões. Você pode ajustar o MTU do EDT para evitar isso. Use a Descoberta de MTU ou a solução alternativa descrita em CTX231821.
- Uma tela cinza ou preta pode aparecer ao iniciar uma sessão de um cliente Windows se a Descoberta de MTU estiver ativada. Para resolver esse problema, atualize para o Workspace app para Windows 2105 ou posterior ou Workspace app para Windows 1912 CU4 ou posterior.
- O fallback para TCP pode falhar em clientes Linux e Android ao se conectar via Citrix Gateway ou Citrix Gateway Service. Isso ocorre quando há uma negociação EDT bem-sucedida entre o cliente e o Gateway, e a negociação EDT falha entre o Gateway e o VDA. Para resolver esse problema, atualize para o Workspace app para Linux 2104 ou posterior e Workspace app para Android 21.5 ou posterior.
- Caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe para conexões que não passam pelo Citrix Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para a versão 2103 ou posterior do VDA.

- Ao usar o Citrix Gateway ou Citrix Gateway Service, caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe. Isso se deve a um problema no Gateway que faz com que o bit Don't Fragment (DF) no cabeçalho dos pacotes EDT não seja propagado. Uma correção para esse problema ainda não está disponível.
- A Descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não conseguem respeitar o bit DF quando o processamento de pacotes está ativado, impedindo que a Descoberta de MTU detecte a fragmentação. Nesta situação, estas são as opções disponíveis:
  - Desativar o processamento de pacotes no modem do usuário.
  - Desative a Descoberta de MTU e use um MTU codificado, conforme descrito em CTX231821.
  - Desative o Adaptive Transport 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.
- Aplicativos publicados não são iniciados para alguns usuários ao se conectar via VPN. Nenhum erro é exibido. Consulte CTX280797 para obter mais detalhes.

Solução de problemas

Para solucionar problemas do Adaptive Transport e do EDT, sugerimos o seguinte:

1. Revise e valide cuidadosamente os requisitos, as considerações e os problemas conhecidos.
2. Verifique se há políticas Citrix no Studio ou GPO que substituem a configuração desejada de **HDX Adaptive Transport**.
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. Inicie uma sessão direta internamente, ignorando o Citrix Gateway, e verifique o protocolo em uso. Se a sessão usar EDT, o VDA estará pronto para usar EDT para conexões externas através do Citrix Gateway.

6. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo Citrix Gateway:
    - Certifique-se de que a Confiabilidade da Sessão esteja ativada
    - Certifique-se de que o Gateway tenha o DTLS ativado
7. Verifique se as regras de firewall apropriadas foram configuradas tanto nos firewalls de rede quanto nos firewalls em execução nas máquinas VDA.
8. 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 VPN, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Para obter informações sobre como resolver esse problema, consulte a seção Descoberta de MTU.

Interoperabilidade com Citrix SD-WAN™

A otimização de WAN do Citrix SD-WAN (WANOP) oferece compactação tokenizada entre sessões (deduplicação de dados), incluindo cache de vídeo baseado em URL, proporcionando uma redução significativa da largura de banda. A redução ocorre se duas ou mais pessoas no local do escritório assistirem ao mesmo vídeo obtido pelo cliente ou transferirem ou imprimirem partes significativas do mesmo arquivo ou documento. Além disso, ao executar os processos de redução de dados ICA e compactação de trabalhos de impressão no appliance da filial, o WANOP oferece descarregamento da CPU do servidor VDA e permite maior escalabilidade do servidor Citrix Virtual Apps and Desktops.

Atualmente, o SD-WAN WANOP não oferece suporte ao EDT. No entanto, não há necessidade de desativar o Adaptive Transport se o SD-WAN WANOP estiver em uso. Quando um usuário inicia uma sessão que passa por um SD-WAN com WANOP ativado, ele define automaticamente a sessão para usar TCP como protocolo de transporte. As sessões não-WANOP continuam a usar EDT sempre que possível.

Canais virtuais Citrix ICA®

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso

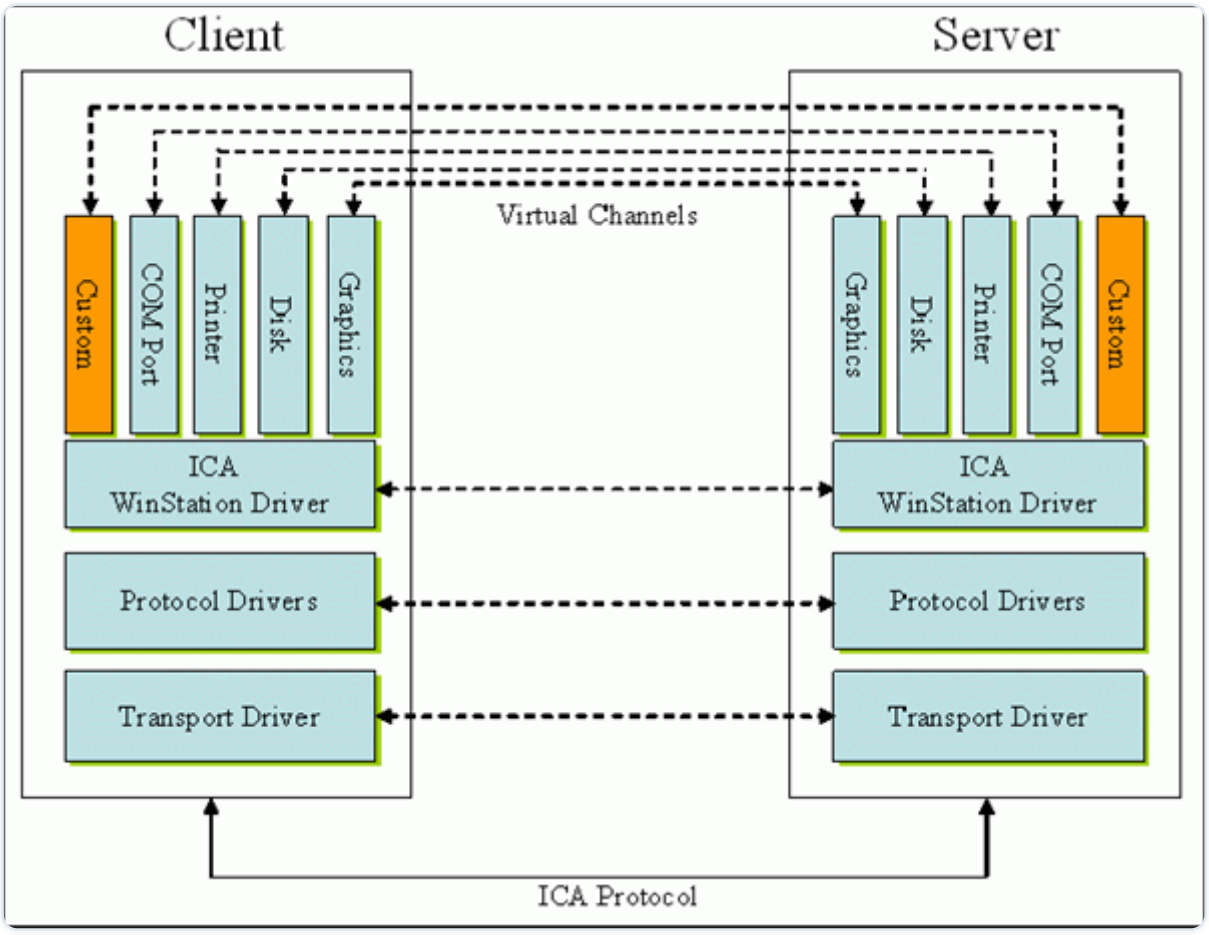
> incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

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. Canais virtuais são uma parte necessária da experiência de computação remota com os servidores Citrix Virtual Apps and Desktops. Canais virtuais são usados para:

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

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



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

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

No lado do cliente, os canais virtuais correspondem a drivers virtuais. Cada driver virtual fornece uma função específica. Alguns são necessários para a operação normal, e outros são opcionais. Os drivers virtuais operam no nível do protocolo da camada de apresentação. Pode haver vários protocolos ativos a qualquer momento, multiplexando canais fornecidos pela camada de protocolo 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
- Áudio do Cliente
- 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 Citrix Workspace app para Windows usam esses arquivos. Eles estão na

> forma de Bibliotecas de Vínculo Dinâmico (modo de usuário) e não de drivers do Windows (modo kernel), exceto para USB Genérico, conforme descrito no canal virtual USB Genérico.

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

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

Compatibilidade de 64 bits

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

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

Canal virtual USB genérico

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

- ctxusbm.sys
- ctxusbr.sys

Como os canais virtuais ICA funcionam

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

Módulos de canal virtual carregados pelo Shell, por exemplo:

- EUEM
- Twain
- Área de transferência

- Multimídia
- Compartilhamento de sessão contínuo
- Fuso horário

Alguns são carregados como modo kernel, por exemplo:

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

Canal virtual gráfico no lado do servidor

A partir do XenApp 7.0 e XenDesktop 7.0, `ctxgfx.exe` hospeda o canal virtual gráfico para sessões baseadas em estação de trabalho e servidor de terminal. `Ctxgfx` hospeda módulos específicos da plataforma que interagem com o driver correspondente (`Icardd.dll` para RDSH e `vdod.dll` e `vidd.dll` para estação de trabalho).

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

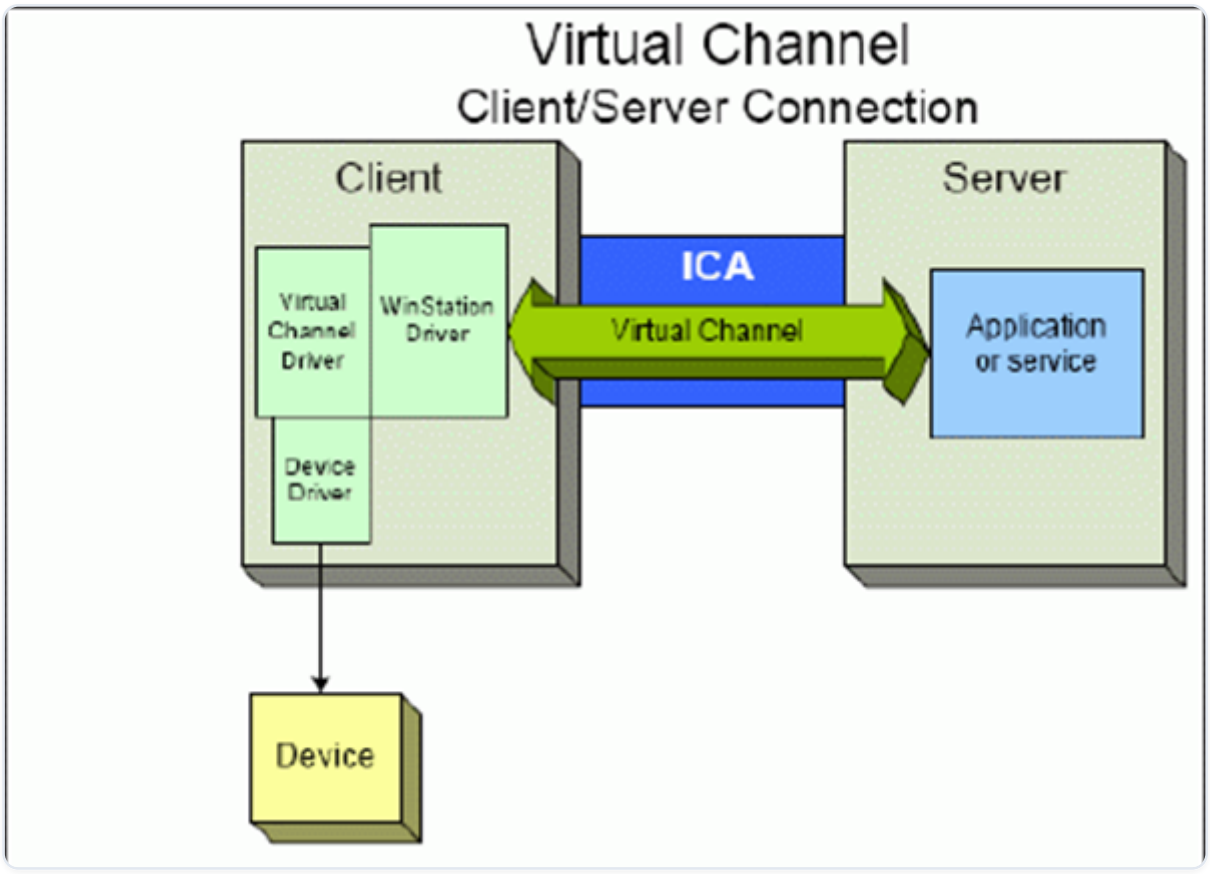
Hospedagem de canais especializados em serviços do Windows

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

- Serviço de Redirecionamento de Dispositivos 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™)

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 é iniciado, obtém um manipular para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.
3. O driver virtual do cliente e o aplicativo do lado do servidor passam dados usando os dois métodos a seguir:

    - Se o aplicativo do servidor tiver dados para enviar ao cliente, os dados serão enviados ao cliente imediatamente. Quando o cliente recebe os dados, o driver WinStation desmultiplexa os dados do canal virtual do fluxo ICA e os passa imediatamente para o driver virtual do cliente.

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

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

Criando seu próprio canal virtual usando o SDK do Canal Virtual

> **Observação:**

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

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

> **Observação:**

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

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

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

> **Importante:**

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

Funcionalidade de passagem de canais virtuais

A maioria dos canais virtuais que a Citrix oferece opera sem modificações ao usar o aplicativo Citrix Workspace para Windows dentro de uma sessão ICA (também conhecida como sessão de passagem). Há considerações ao usar o cliente em saltos adicionais.

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
- Passagem transparente de chave
- Twain

Devido à natureza inerente da latência e a fatores como compressão, 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 em uma sessão ICA em um servidor Citrix Virtual Desktops (também conhecido como sessão de passagem).

Especificamente, no servidor Citrix Virtual Desktops, existe um hook VDA que executa **picaPassthruHook**. Este hook faz o cliente pensar que está sendo executado em um servidor CPS e 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 a segurança do uso é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança localizadas em todo este documento.

Melhores práticas

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

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

Nomeando os Canais Virtuais:

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

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

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

Suporte a Double-Hop:

CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
Áudio	Não
Redirecionamento de Conteúdo do Navegador	Não
CDM	Sim
CEIP	Não
Área de Transferência	Sim
Continuum (MRVC)	Não
Control VC	Sim

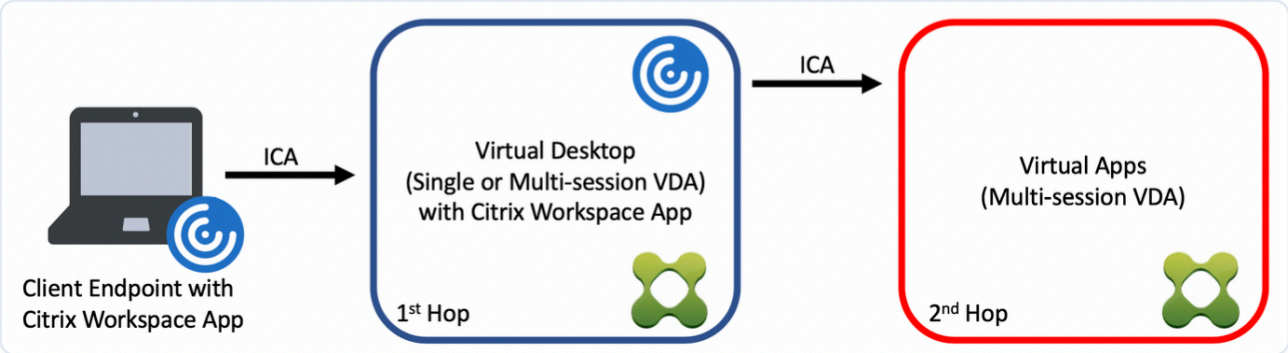
CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
Redirecionamento de Vídeo HTML5 (v1)	Sim
Teclado, Mouse	Sim
Multitoque	Não
NSAPVC	Não
Impressão	Sim
SensVC	Não
Smartcard	Sim
Twain	Sim
VC USB	Sim
Dispositivos WAYCOM - K2M usando VC USB	Sim
Compressão de Vídeo da Webcam	Sim
Redirecionamento de Mídia do Windows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

Consulte também

- SDK de Canal Virtual ICA
- A Citrix Developer Network é o lar de todos os recursos técnicos e discussões envolvendo o uso de SDKs 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 ocorrem discussões técnicas sobre cada um dos SDKs Citrix.

Salto duplo no Citrix Virtual Apps and Desktops™

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



Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktop executado em um VDA de SO de sessão única (conhecido como VDI) ou em um VDA de SO de 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 do Citrix Virtual Apps™. Isso é considerado o segundo salto.

Você pode usar um modelo de implantação de salto duplo para suportar vários casos de uso. O caso em que os ambientes 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™, suportam salto duplo.

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

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

Em ambientes onde o primeiro salto envolve uma solução de desktop virtual de terceiros (não-Citrix) em combinação com uma sessão do Citrix Virtual Apps, o suporte é limitado ao ambiente 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 do HDX 3D Pro, a Citrix recomenda fortemente que todos os aplicativos que exigem aceleração gráfica sejam executados localmente no primeiro salto com os recursos de GPU apropriados disponíveis para o VDA.

Latência

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

Multimídia

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

Redirecionamento de dispositivo USB

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

PRIMEIRO SALTO (VDI OU DESKTOP PUBLICADO)	SEGUNDO SALTO (APLICATIVOS VIRTUAIS)	NOTAS DE SUPORTE
Otimizado	Otimizado	Recomendado (com base no suporte ao dispositivo). Por exemplo, armazenamento em

PRIMEIRO SALTO (VDI OU DESKTOP PUBLICADO)	SEGUNDO SALTO (APLICATIVOS VIRTUAIS)	NOTAS DE SUPORTE
		massa USB, scanners TWAIN, webcam, áudio.
Genérico	Genérico	Para dispositivos onde a opção otimizada não está disponível.
Genérico	Otimizado	Embora tecnicamente possível, é recomendado usar o modo otimizado em ambos os saltos quando o suporte ao dispositivo estiver disponível.
Otimizado	Genérico	Não suportado

Observação:

Devido à natureza inerentemente comunicativa 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 é especialmente importante em cenários de salto duplo.

Exceções de suporte

As sessões de salto duplo suportam a maioria dos recursos e capacidades HDX, com exceção do seguinte:

- Redirecionamento de conteúdo do navegador(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
- Acesso a Aplicativos Locais
- Pacote de Otimização em Tempo Real para Skype for Business
- Otimização para Microsoft Teams

Instalar e configurar

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

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

Preparar

Revise Preparar para instalar e conclua todas as tarefas necessárias.

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

Instalar componentes principais

Instale o Delivery Controller, Citrix 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 automaticamente guiado para criar um site.

Instalar um ou mais Virtual Delivery Agents (VDAs)

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

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

Para uma implantação de Acesso Remoto a PC, instale um VDA para 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). (Preparar 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 na criação de VMs.

Criar um grupo de entrega

Depois de criar seu primeiro catálogo de máquinas no 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.

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 Studio
- 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.

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 no Active Directory. Você também pode usar os scripts para gerenciar imagens usadas pelo Machine Creation Services (MCS) e Citrix Provisioning (anteriormente Provisioning Services). Para obter detalhes, consulte Instalar VDAs usando scripts.

Informações a serem revisadas antes da instalação

- Visão geral técnica: Se você não estiver familiarizado com o produto e seus componentes.
- Segurança: Ao planejar seu ambiente de implantação.
- Problemas conhecidos: Problemas que você pode encontrar nesta versão.
- Bancos de dados: Saiba mais sobre os bancos de dados do sistema e como configurá-los. Durante a instalação do Controller, você pode instalar o SQL Server Express para usar como banco de dados do site. Você configura a maioria das informações do banco de dados ao criar um site, após instalar os componentes principais.
- Acesso Remoto para PC: Se você estiver implantando um ambiente que permite que seus usuários acessem suas máquinas físicas no escritório remotamente.
- Conexões e recursos: Se você estiver usando um hipervisor ou outro serviço para hospedar ou provisionar VMs para aplicativos e desktops. Você pode configurar a primeira conexão ao criar um site (após instalar os componentes principais). Configure seu ambiente de virtualização antes disso.
- Microsoft System Center Configuration Manager: Se você estiver usando o ConfigMgr para gerenciar o acesso a aplicativos e desktops, ou se estiver usando o recurso Wake on LAN com o Acesso Remoto para PC.
- **Conexões de host de nuvem pública:** Se você tiver a Licença de Direitos Híbridos, poderá criar conexões de host com a nuvem pública. Para obter informações relacionadas à Licença de Direitos Híbridos, consulte Direitos Híbridos. Para obter informações relacionadas ao direito à nuvem pública e o motivo dessa alteração, consulte CTX270373.

Onde instalar os componentes

Revise os Requisitos do sistema para plataformas, sistemas operacionais e versões compatíveis. Os pré-requisitos dos componentes são instalados automaticamente, exceto conforme observado. Consulte a documentação do Citrix StoreFront e do Citrix License Server para suas plataformas e pré-requisitos compatíveis.

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 sistema operacional não oferece uma interface gráfica, então instale o Studio e outras ferramentas em outro lugar e, em seguida, aponte-os para o servidor Controller.

Você pode instalar um Delivery Controller™ e um VDA para SO multi-sessão no mesmo servidor. Inicie o instalador e selecione o Delivery Controller (além de quaisquer outros componentes principais que você deseja nessa máquina). Em seguida, inicie o instalador novamente e selecione o **Virtual Delivery Agent** para SO multi-sessão.

Certifique-se de que cada sistema operacional tenha as atualizações mais recentes.

Certifique-se de que todas as máquinas tenham os relógios do sistema sincronizados. A infraestrutura Kerberos que protege a comunicação entre as máquinas requer sincronização.

Com os Citrix Hypervisors, o estado de energia da máquina virtual pode aparecer como desconhecido, mesmo que pareça registrado. Para resolver esse problema, edite o valor da chave de registro `HostTime` para desabilitar a sincronização de tempo com o host:

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

> **Dica:**

> O valor padrão é `HostTime="UTC"`. Altere este valor para algo diferente de UTC, por exemplo, `Local`. Essa alteração desabilita efetivamente a sincronização de tempo com o host.

> Orientações de otimização para máquinas Windows 10 de sessão única estão disponíveis em CTX216252.

Onde NÃO instalar componentes:

- Não instale nenhum componente em um controlador de domínio do Active Directory.
- Não é suportada a instalação de um Controller em um nó em uma instalação de cluster do SQL Server, instalação de espelhamento do SQL Server ou em um servidor executando o Hyper-V.

Se você tentar instalar ou atualizar um VDA em um SO Windows que esta versão do produto não suporta, uma mensagem o guiará para um artigo que descreve as opções.

Requisitos de permissão e Active Directory

Você deve ser um usuário de domínio e um administrador local nas máquinas onde você está instalando os componentes.

Para usar um instalador VDA autônomo, você deve ter privilégios administrativos elevados ou usar **Executar como administrador**.

Configure seu domínio do Active Directory antes de iniciar uma instalação.

- Requisitos do sistema lista os níveis funcionais do Active Directory suportados. Active Directory 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 obter mais informações:

- Melhores práticas de segurança
- Administração delegada
- Documentação da Microsoft para configuração do Active Directory

Orientação de instalação, considerações e melhores práticas

Durante a instalação de qualquer componente

- Ao instalar ou atualizar um Delivery Controller, Studio, License Server ou Director a partir da mídia do produto completo, se o instalador Citrix detectar que uma reinicialização está pendente de uma instalação anterior do Windows na máquina, o instalador para com o código de saída/retorno 9. Você será solicitado a reiniciar a máquina.

  Esta não é uma reinicialização forçada do Citrix. É devido a outros componentes instalados anteriormente na máquina. Se isso ocorrer, reinicie a máquina e, em seguida, inicie o instalador Citrix novamente.

  Ao usar a interface de linha de comando, você pode impedir a verificação da reinicialização pendente incluindo a opção `/no_pending_reboot_check` no comando.
- Normalmente, 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 dados do 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.
- O Google Analytics é coletado (e posteriormente carregado) automaticamente quando você instala (ou atualiza) o Studio. Após a instalação do Studio, você pode alterar essa configuração

com a chave 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 à Citrix.

Durante a instalação do VDA

- O aplicativo Citrix Workspace™ 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 aplicativo Citrix Workspace para Windows e outros aplicativos Citrix Workspace no site da Citrix. Alternativamente, você pode disponibilizar esses aplicativos Citrix Workspace a partir do 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.

Ferramentas de suporte do VDA

Cada instalador de VDA inclui um MSI de suporte que contém ferramentas Citrix para verificar o desempenho do VDA, como sua saúde geral e a qualidade das conexões. Habilite ou desabilite a instalação deste MSI na página **Componentes Adicionais** da interface gráfica do instalador do VDA. Na linha de comando, você pode desabilitar a instalação com a opção `/exclude "Citrix Supportability Tools"`.

Por padrão, o MSI de suporte é instalado em `c:\Program Files (x86)\Citrix\Supportability Tools\`. Você pode alterar este local na página **Componentes** da interface gráfica do instalador do VDA, ou com a opção de linha de comando `/installdir`. Lembre-se de que alterar o local o altera para todos os componentes VDA instalados, não apenas para as ferramentas de suporte.

Ferramentas atuais no MSI de suporte:

- Citrix Health Assistant: Para obter detalhes, consulte CTX207624.
- Utilitário de Limpeza do VDA: Para obter detalhes, consulte CTX209255.

Se você não instalar as ferramentas ao instalar o VDA, o artigo CTX conterá um link para o pacote de download atual.

Reinicializações após e durante a instalação do VDA

É necessário reiniciar ao final da instalação do VDA. Essa reinicialização ocorre automaticamente por padrão.

Ao atualizar um VDA para a versão 7.17 (ou uma versão posterior compatível), ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Para minimizar o número de reinicializações necessárias durante a instalação do VDA:

- Certifique-se de que uma versão compatível do .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas com SO Windows multi-sessão, instale e habilite os serviços de função RDS antes de instalar o VDA.

Se você não instalar esses pré-requisitos antes de instalar o VDA:

- Se você estiver usando a interface gráfica ou a interface de linha de comando sem a opção `/noreboot`, a máquina reinicia automaticamente após a instalação do pré-requisito.

- Se você estiver usando a interface de linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Ao atualizar um VDA para a versão 7.17 ou uma versão posterior compatível, ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Restaurar em caso de falha na instalação ou atualização

> **Observação:**
>
> Este recurso está disponível para VDAs de sessão única e multi-sessão.
>
> Se uma instalação ou atualização de VDA de sessão única falhar, e o recurso "restaurar em caso de falha" estiver habilitado, a máquina é retornada a um ponto de restauração que foi definido antes do início da instalação ou atualização.

Se uma instalação ou atualização de VDA multi-sessão falhar, e o recurso “restaurar em caso de falha” estiver ativado, 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 ativado, o instalador cria um backup do servidor antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado de backup. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração. O tempo para criar o backup do servidor é baseado no tamanho do backup necessário e na quantidade de recursos disponíveis para o servidor. O backup é armazenado em *C:\WindowsImageBackup\servername*.

Por padrão, este recurso está desabilitado.

Se você planeja habilitar este recurso, certifique-se de que a restauração do sistema não esteja desabilitada por meio de uma configuração de GPO (`Computer Configuration > Administrative Templates > System > System Restore`).

Observação:

Esta configuração de GPO não se aplica à restauração de um VDA multi-sessão.

Para ativar este recurso ao instalar ou atualizar um VDA de sessão única ou multi-sessão:

- Ao usar a interface gráfica de um instalador VDA (como usando **Autostart** ou o comando `XenDesktopVDASetup.exe` sem quaisquer opções de restauração ou silenciosas), selecione a caixa de seleção **Habilitar restauração automática se a atualização falhar** na página **Resumo**.

  Se a instalação/atualização for concluída com sucesso, o ponto de restauração/backup não é usado, mas é retido.
- Execute um instalador VDA com a opção `/enablerestore` ou `/enablerestorecleanup` usando a linha de comando.
  - Se você usar a opção `/enablerestorecleanup`, e a instalação/atualização for concluída com sucesso, o ponto de restauração/backup do servidor será removido automaticamente.
  - Se você usar a opção `/enablerestore`, e a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será retido.

Instaladores

Instalador completo do produto

Usando o instalador completo do produto fornecido na ISO, você pode:

- Instalar, atualizar ou remover componentes principais: Delivery Controller, Studio, Director e License Server.
- Instalar ou atualizar o StoreFront.
- Instalar ou atualizar VDAs do Windows para sistemas operacionais de sessão única ou multi-sessão.
- Instalar o componente `UpsServer` do Universal Print Server em seus servidores de impressão.
- Instalar o Federated Authentication Service.
- Instalar o Session Recording.

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 a ISO completa do produto. Eles acomodam mais facilmente implantações que:

- Usam pacotes de Distribuição Eletrônica de Software (ESD) que são preparados ou copiados localmente
- Possuem máquinas físicas
- Ter escritórios remotos

Por padrão, os arquivos nos VDAs autônomos de autoextração são extraídos para a pasta **Temp**. Mais espaço em disco é necessário na máquina ao extrair para a pasta **Temp** do que ao usar o instalador do produto completo. No entanto, os arquivos extraídos para a pasta **Temp** são automaticamente excluídos após a conclusão da instalação. Alternativamente, você pode usar o comando `/extract` com um caminho absoluto.

Três instaladores VDA autônomos estão disponíveis para download.

VDAServerSetup.exe:

Instala um VDA para SO de várias sessões. Ele suporta todas as opções de VDA para SO de várias sessões 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 otimizado para implantações de Acesso Remoto a PC ou instalações VDI principais. O Acesso Remoto a PC usa máquinas físicas. As instalações VDI principais são VMs que não estão sendo usadas como uma imagem. Ele instala apenas os serviços principais necessários para conexões VDA nessas implantações. Portanto, ele suporta apenas um subconjunto das opções válidas com os instaladores do produto completo ou `VDAWorkstationSetup.exe`.

Este instalador não instala nem contém os componentes usados para:

- App-V.
- Gerenciamento de Perfis. Excluir o Gerenciamento de Perfis Citrix da instalação afeta as exibições do Citrix Director. Para obter detalhes, consulte Instalar VDAs.
- Serviço de Identidade da Máquina.
- Ferramentas de Suporte da Citrix.
- Citrix Files para Windows.
- Citrix Files para Outlook.
- Agente Citrix WEM.

O instalador `VDAWorkstationCoreSetup.exe` não instala nem contém um aplicativo Citrix Workspace para Windows.

Usar `VDAWorkstationCoreSetup.exe` é equivalente a usar o instalador do produto completo ou `VDAWorkstationSetup` para instalar um VDA de SO de sessão única e uma das seguintes opções:

- Na interface gráfica: Selecionar a opção Acesso Remoto para PC na página **Ambiente**.
- Na interface de linha de comando: Especificar a opção `/remotepc`.
- Na interface de linha de comando: Especificar `/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 do produto completo. 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 às versões 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 = Sucesso Parcial

- 3 = Sucesso Parcial e Reinicialização Necessária
- 4 = Falha e Reinicialização Necessária
- 5 = UsuárioCancelou
- 6 = ArgumentoDeLinhaDeComandoAusente
- 7 = VersaoMaisRecenteEncontrada
- 8 = SucessoReinicializacaoNecessaria
- 9 = ReinicializacaoPorBloqueioDeArquivo
- 10 = Abortado
- 11 = MidiaComFalha
- 12 = LicencaComFalha
- 13 = Falha na Verificação Prévia
- 14 = Verificação de Reinicialização Pendente Abortada
- -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 a instalação de um pré-requisito de função RDS em um servidor). Uma instalação de VDA é considerada bem-sucedida somente depois que todos os pré-requisitos e componentes selecionados são instalados e a máquina é reiniciada após a instalação.

Alternativamente, você pode encapsular sua instalação em scripts CMD (que retornam códigos de saída da Microsoft) ou alterar os códigos de sucesso em seu pacote do Configuration Manager.

Configurar um Servidor de Licenças RDS da Microsoft para cargas de trabalho do Windows Server

Este produto acessa os recursos de sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2016. Isso geralmente requer uma licença de acesso 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 Licencie 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 de 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 acessar este servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Especifique o Modo de Licenciamento da Área de Trabalho Remota para um Servidor Host de Sessão RD.

As cargas de trabalho do Windows 10 exigem a ativação apropriada da licença do Windows 10. Recomendamos que você siga a documentação da Microsoft para ativar as cargas de trabalho do Windows 10.

Ambientes de nuvem do Microsoft Azure Resource Manager

Siga as orientações deste artigo ao usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™.

Presumimos que você esteja familiarizado 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/>`

Provisionamento sob demanda do Azure

Com o provisionamento sob demanda do Azure, as VMs são criadas somente quando o Citrix Virtual Apps and Desktops inicia uma ação de ligar, após a conclusão do provisionamento.

Ao usar o MCS para criar catálogos de máquinas no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz seus custos de armazenamento
- Oferece criação de catálogo mais rápida

Ao criar um catálogo MCS, o portal do Azure exibe o grupo de segurança de rede, as interfaces de rede, as imagens base e os discos de identidade nos grupos de recursos.

O portal do Azure não mostra uma VM até que o Citrix Virtual Apps and Desktops inicie uma ação de ligar para ela. Existem dois tipos de máquinas com as seguintes diferenças:

- Para uma máquina agrupada, o disco do sistema operacional e o cache de write-back existem apenas quando a VM existe. Ao desligar uma máquina agrupada no console, a VM não fica visível no portal do Azure. Há uma economia significativa de custos de armazenamento se você desligar as máquinas rotineiramente (por exemplo, fora do horário de trabalho).
- Para uma máquina dedicada, o disco do sistema operacional é criado na primeira vez que a VM é ligada. A VM no portal do Azure permanece 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.

Conexão com o Azure Resource Manager

(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos das conexões do Azure Resource Manager.

Considerações:

- A Citrix® recomenda usar a Entidade 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 tem efeitos não intencionais 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.

Você pode estabelecer uma conexão de host com o Azure de duas maneiras:

- autenticar no Azure para criar uma entidade de serviço.
- Use os detalhes de uma entidade de serviço criada anteriormente para se conectar ao Azure.

Criar um principal de serviço

> **Importante:**

> Este recurso ainda não está disponível para assinaturas do Azure China e Azure Alemanha.

> Antes de começar, autenticar no Azure. Certifique-se de que:

- Você tem uma conta de usuário no locatário do Azure Active Directory da sua assinatura.

- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativo para autenticação. Essas permissões podem ser revogadas depois que você cria a conexão de host. Para obter mais informações sobre funções, consulte Funções internas do Azure AD.

Quando você autenticar no Azure para criar uma entidade de serviço, um aplicativo é registrado no Azure. Uma chave secreta (segredo do cliente) é criada para o aplicativo registrado. O aplicativo registrado usa o segredo do cliente para autenticar no Azure AD. Certifique-se de alterar o segredo do cliente antes que ele expire. Você recebe um alerta no console antes que a chave secreta expire.

Para autenticar no Azure para criar uma entidade de serviço, conclua as seguintes etapas 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 sua ID de assinatura do Azure e um nome para a conexão. Depois de inserir a 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 uma entidade de serviço que permite gerenciar recursos do Azure em nome do usuário especificado.
7. Depois de selecionar **Aceitar**, você retorna à página **Conexão** no assistente.

> **Observação:**
>
> Depois de autenticar com sucesso no Azure, os botões **Criar novo** e **Usar existente** desaparecem. O texto **Conexão bem-sucedida** aparece, com uma marca de seleção verde, indicando a conexão bem-sucedida 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 incluem 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.

Use os detalhes de um principal de serviço criado anteriormente para se conectar ao Azure

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

Pré-requisitos:

- **SubscriptionId:** `SubscriptionID` do Azure Resource Manager para a assinatura onde você deseja provisionar VDAs.
- **ActiveDirectoryID**: ID de locatário do aplicativo que você registrou no Azure AD.
- **ApplicationName:** Nome do aplicativo a ser criado no Azure AD.

Para criar um principal de serviço:

1. Conecte-se à sua assinatura do Azure Resource Manager.

   ```
   Connect-AzAccount
   ```

2. Selecione a assinatura do Azure Resource Manager onde você deseja criar a entidade de serviço.

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

3. Crie o aplicativo em seu locatário do AD.

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

4. Crie uma entidade de serviço.

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

5. Atribua uma função à entidade de serviço.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

6. Na janela de saída do console do PowerShell, anote o ApplicationId. Você fornece esse ID ao criar a conexão de host.

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 sua ID de assinatura do Azure e um nome para a conexão.

> **Nota:**

> O nome da conexão pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco 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 a ID do Diretório (locatário) do aplicativo que você registrou no Azure AD.
   - **ID do Aplicativo**. Insira a 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 receberá um alerta no console antes que a chave secreta expire. No entanto, se a chave secreta expirar, você receberá erros.

     > **Nota:**
     >
     > Para fins de segurança, o período de expiração não pode ser superior a dois anos a partir de agora.

   - **URL de autenticação**. Este campo é preenchido automaticamente e não é editável.
   - **URL de gerenciamento**. Este campo é preenchido automaticamente e não é editável.
   - **Sufixo de armazenamento**. Este campo é preenchido automaticamente e não é editável.

     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 prosseguir 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, emparelhar o 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.

Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager

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. Para obter informações gerais sobre imagens, consulte Criar catálogos de máquinas.

Limitação do Azure

O Azure Resource Manager limita as solicitações para assinaturas e locatários, roteando o tráfego com base em limites definidos, adaptados às necessidades específicas do provedor. Consulte Limitação de solicitações do Resource Manager no site da Microsoft para obter mais informações.

Existem limites para assinaturas e locatários, onde o gerenciamento de muitas máquinas pode se tornar problemático. Por exemplo, uma assinatura contendo muitas máquinas pode apresentar problemas de desempenho relacionados a operações de energia.

> **Dica:**
>
> Para obter mais informações, consulte Melhorando o desempenho do Azure com o Machine Creation Services.
>
> Para ajudar a mitigar esses problemas, você pode remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

Recomendamos as seguintes configurações ideais ao ligar ou desligar VMs em grandes assinaturas, por exemplo, aquelas que contêm 1.000 VMs:

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

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`.

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 completo para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar 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 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 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 para usar 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"
```

```
            }

        ],
```

COMO CRIAR MÁQUINAS USANDO DISCOS DE SO EFÊMEROS

Os discos de SO efêmeros são controlados com base na propriedade `UseEphemeralOsDisk` no parâmetro `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.

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 habilitados 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`) definidos como **true** em `New-ProvScheme` ou `Set-ProvScheme` falham com uma mensagem de erro apropriada.
- Para catálogos de máquinas existentes criados com ambas as funcionalidades ativadas, você ainda pode:
    - atualizar um catálogo de máquinas.

- adicionar ou excluir VMs.
- excluir um catálogo de máquinas.

Criptografia do lado do servidor do Azure

O Citrix Virtual Apps and Desktops e o Citrix DaaS suportam chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure através do Azure Key Vault. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados do seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Criptografia do lado do servidor do Armazenamento em Disco do Azure.

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco é criptografado, você altera a chave atual no `DiskEncryptionSet`. Todos os recursos associados a esse `DiskEncryptionSet` mudam para serem criptografados com a nova chave.
- Quando você desativa ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja ativada novamente ou você atribua uma nova chave. Qualquer catálogo que use a chave não pode ser ligado, e você não pode adicionar VMs a ele.

Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente

Considere o seguinte ao usar este recurso:

- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- 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 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 que você selecionar 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.

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 haja 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.

Galeria de Imagens Compartilhadas do Azure

Use a Galeria de Imagens Compartilhadas do Azure como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação de discos 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 funciona apenas com discos gerenciados. Não está disponível para catálogos de máquinas legados.

> Para obter mais informações, consulte Visão geral da galeria de imagens compartilhadas do Azure.

Configurar a Galeria de Imagens Compartilhadas

Use o comando `New-ProvScheme` para criar um esquema de provisionamento com suporte à Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para habilitar ou desabilitar esse recurso para um esquema de provisionamento e para alterar a taxa de réplica e os valores máximos de réplica.

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para oferecer suporte ao recurso 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 da 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 de réplicas atual inalterada.

> **Dica:**
>
> Ao usar a Galeria de Imagens Compartilhadas para armazenar uma imagem publicada para catálogos provisionados por MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na taxa de 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. A reinicialização das máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Imagens Compartilhadas e todas

as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente em algumas horas.

CASO DE USO: CONVERTENDO UM CATÁLOGO DA GALERIA DE IMAGENS COMPARTILHADAS EM UM CATÁLOGO DE INSTANTÂNEOS

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

Dica:

Ao contrário da atualização de um instantâneo para um catálogo da Shared Image Gallery, 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 Shared Image Gallery: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Depois que o comando `Set-ProvScheme` for concluído, o instantâneo da imagem ainda não terá sido criado. Uma vez que o catálogo é configurado para não usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada como um instantâneo. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o instantâneo e todas as máquinas recém-provisionadas são criadas a partir do instantâneo. Reiniciar as máquinas as atualiza, momento em que os dados personalizados da máquina são atualizados para refletir que `UseSharedImageGallery` está definido como **False**. Os ativos antigos da Shared Image Gallery (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.

Configurando Zonas de Disponibilidade via PowerShell

Usando o PowerShell, você pode visualizar os itens de inventário de oferta usando `Get-Item`. Por exemplo, para visualizar a oferta de serviço `Standard_B1ls` da *região Leste dos EUA*:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

Para visualizar as zonas, use o parâmetro `AdditionalData` para o item:

`$serviceOffering.AdditionalData`

Se as Zonas de Disponibilidade não forem especificadas, não haverá alteração na forma como as máquinas são provisionadas.

Para configurar Zonas de Disponibilidade via PowerShell, use a propriedade personalizada **Zones** disponível com a operação `New-ProvScheme`. A propriedade **Zones** define uma lista de Zonas de Disponibilidade para provisionar máquinas. Essas zonas podem incluir uma ou mais Zonas de Disponibilidade. Por exemplo, `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` para as Zonas 1 e 3.

Use o comando `Set-ProvScheme` para atualizar as zonas de um esquema de provisionamento.

Se uma zona inválida for fornecida, o esquema de provisionamento não será atualizado e uma mensagem de erro aparecerá fornecendo instruções sobre como corrigir o comando inválido.

> **Dica:**

> Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro relevante aparecerá.

Disco efêmero do Azure

Discos efêmeros do Azure permitem que você reutilize o cache ou 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.

> **Observação:**

> Catálogos persistentes não suportam discos de SO efêmeros.

> Discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Shared Image Gallery. Para obter mais informações, consulte Galeria de imagens compartilhadas do Azure.

Usando o PowerShell para configurar um disco efêmero

Para configurar um disco de SO efêmero do Azure para um catálogo, use o parâmetro `UseEphemeralOsDisk` em `Set-ProvScheme`. Defina o valor do parâmetro `UseEphemeralOsDisk` como **true**.

> **Observação:**

> Para usar este recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

> Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

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 possuem 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.

Preservando uma máquina virtual provisionada ao reiniciar

Escolha se deseja preservar uma máquina virtual provisionada ao reiniciar. Use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provisionada persiste quando reiniciada. Defina a propriedade `PersistVm` como **true** para manter uma máquina virtual quando desligada, ou defina a propriedade como **false** para garantir que a máquina virtual não seja preservada quando desligada.

Observação:

A propriedade `PersistVm` aplica-se 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 gravação de volta definindo `PersistVM` como **true**:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
```

```
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

Dica:

A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco do SO deve ser persistido. Para preservar uma máquina virtual provisionada, preserve o disco do SO primeiro. Você não pode excluir o disco do SO sem antes excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem especificar o parâmetro `PersistVm`.

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 gravação. Para um catálogo normal, `StorageType` é necessário. Se `WBCDiskStorageType` não for configurado, `StorageType` será usado como padrão para `WBCDiskStorageType`.

> Se WBCDiskStorageType não estiver configurado, então StorageType é usado como padrão para WBCDiskStorageType

Configurando tipos de armazenamento

Para configurar tipos de armazenamento para VM, use o parâmetro `StorageType` em `New-ProvScheme`. Defina o valor do parâmetro `StorageType` para um dos tipos de armazenamento suportados.

A seguir, um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />
```

```
</CustomProperties>'
```

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 do PowerShell `TemplateIsWindowsTemplate` são derivadas da API do Azure. Em alguns casos, este campo pode estar vazio. Por exemplo, um instantâneo de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de SO não pode ser recuperado de um instantâneo.

Por exemplo, defina o parâmetro `AdditionData` da VM do Azure como **True** para o tipo de SO Windows usando 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
```

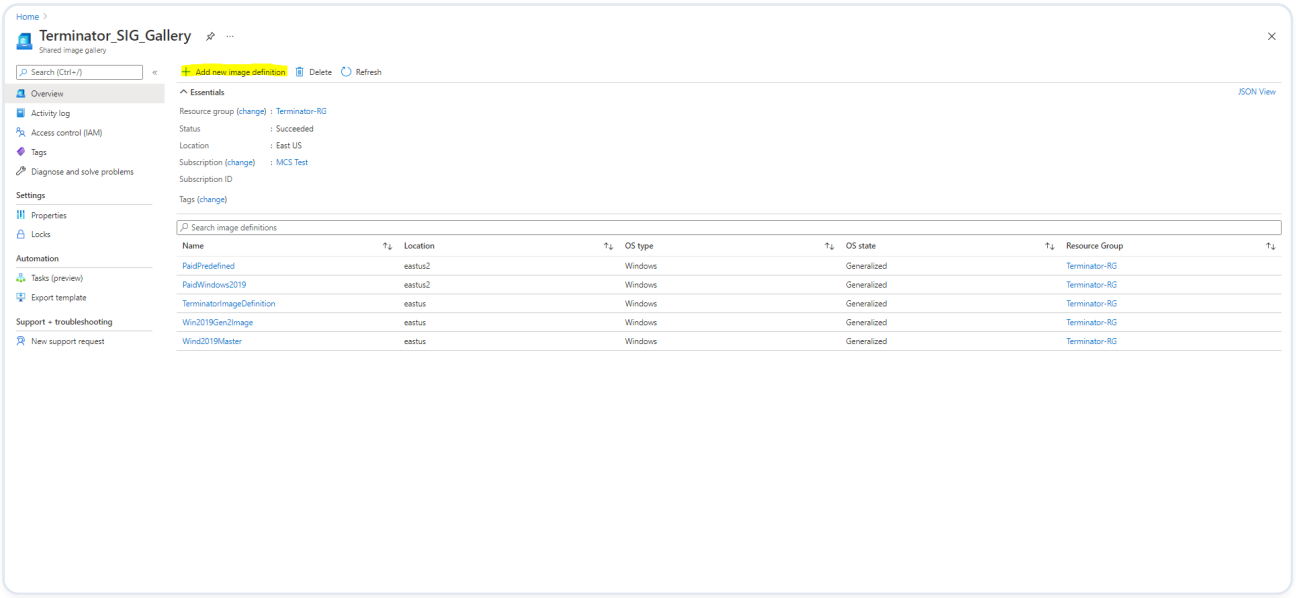
Azure Marketplace

O Citrix Virtual Apps and Desktops e o Citrix DaaS suportam o uso de uma imagem mestre no Azure que contém informações de plano para criar um catálogo de máquinas. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**
>
> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não anexam informações de plano. O recurso Citrix DaaS™ é para imagens pagas.

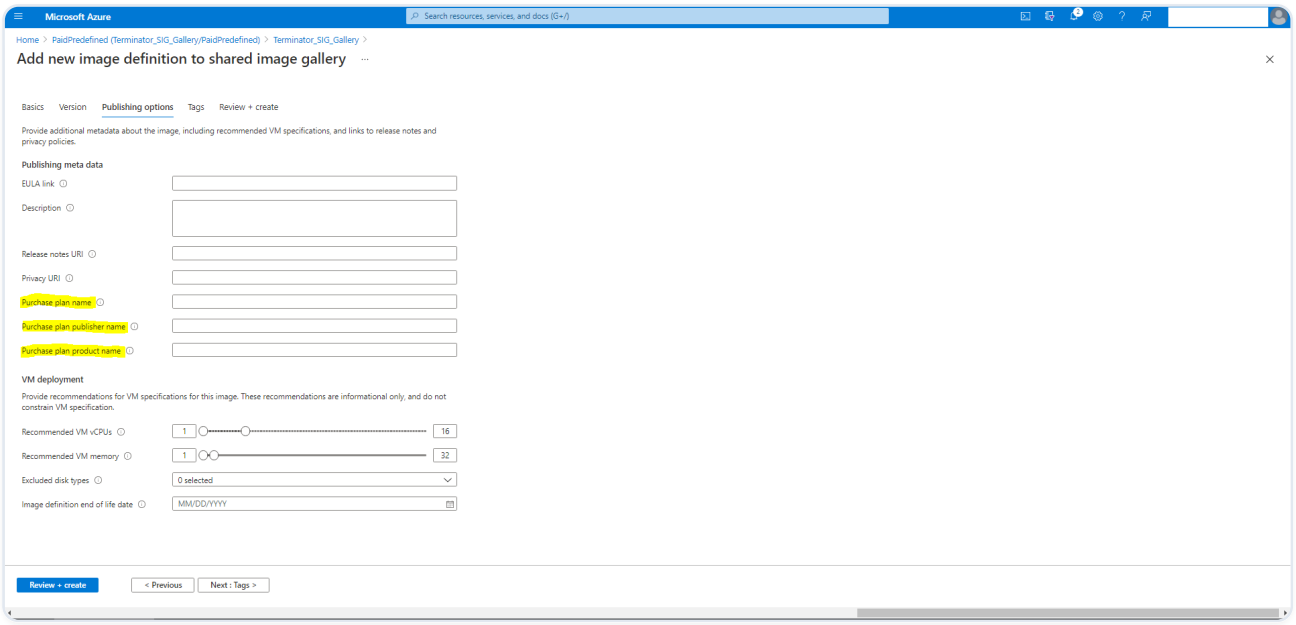
Certifique-se de que a imagem criada na Galeria de Imagens Compartilhadas contenha informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Citrix 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.

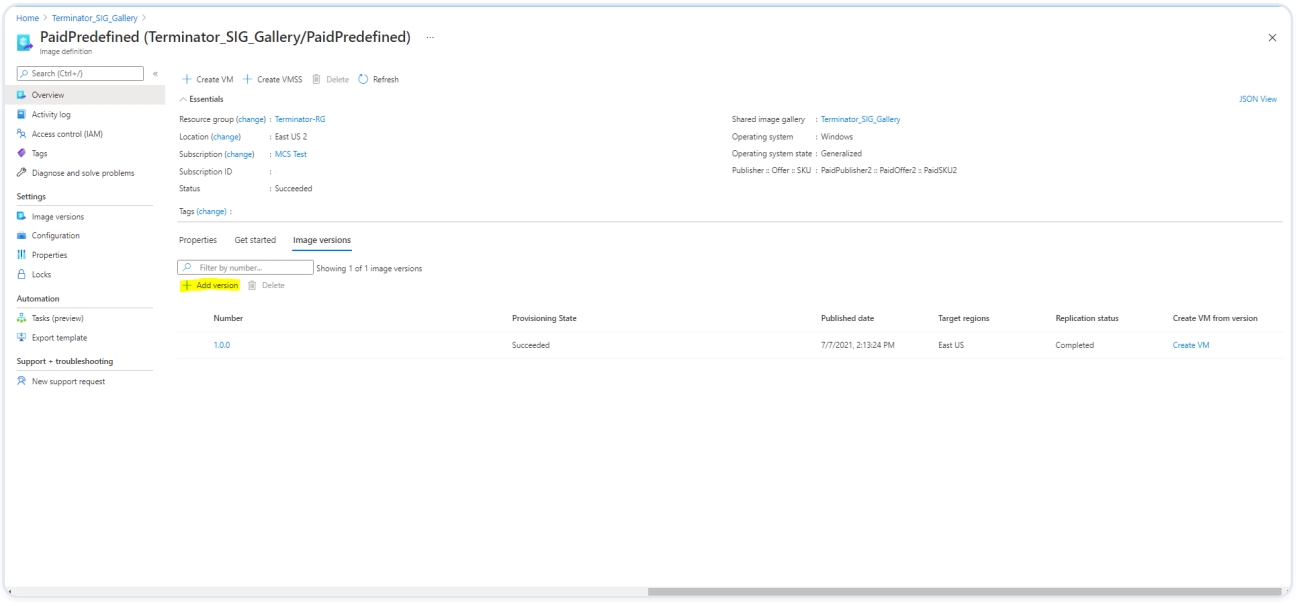


Na página **Opções de publicação**, verifique as informações do plano de compra.

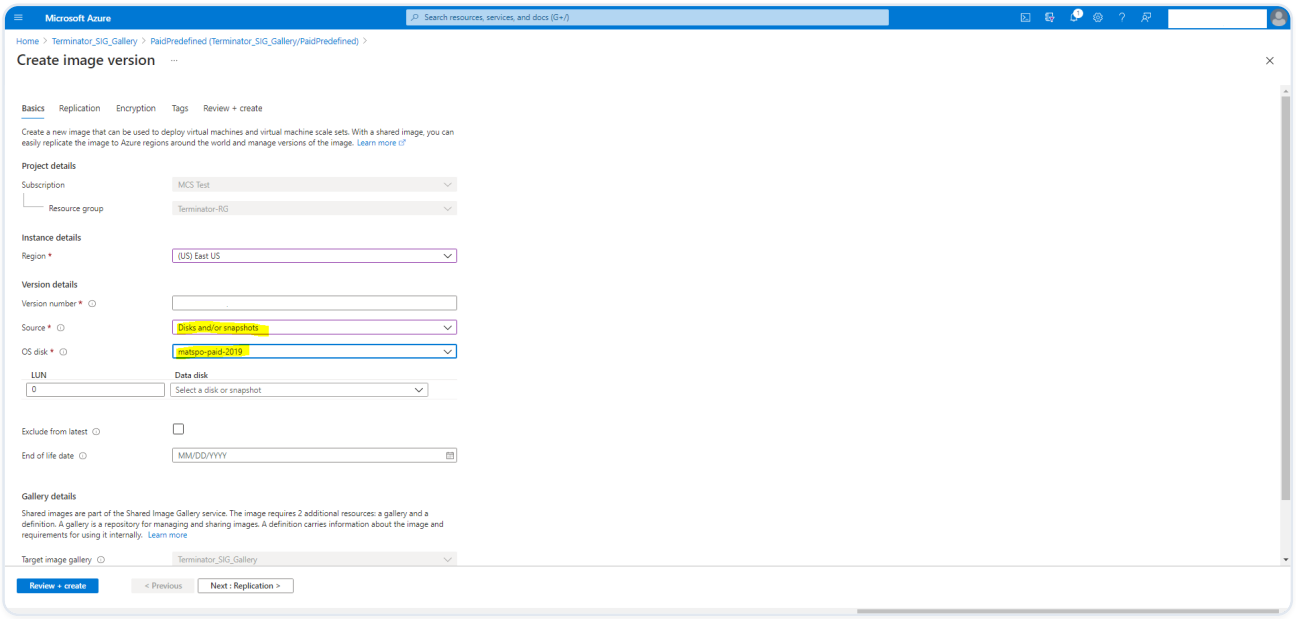
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. A falha ao preencher as informações do plano de compra pode fazer com que o processo de catálogo de máquinas falhe.



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:



Sobre as permissões do Azure

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

Permissões mínimas

As permissões mínimas oferecem melhor controle de segurança. No entanto, novos recursos que exigem permissões adicionais falharão 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 da conexão de hospedagem.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",
```

```
"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

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

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

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- 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. Instantâneos ou VHD estiverem 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 pelo 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 a host dedicado do Azure:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- Se você usar Criptografia do Lado do Servidor (SSE) com Chaves Gerenciadas pelo Cliente (CMK):

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

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

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",
```

- 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 conjunto de permissões a seguir 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",
```

Mais informações

- 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 de virtualização Microsoft System Center Virtual Machine Manager

Siga esta orientação se você usar o Hyper-V com o Microsoft System Center Virtual Machine Manager (VMM) para fornecer máquinas virtuais.

Esta versão oferece suporte às versões do VMM listadas em Requisitos do sistema.

> **Observação:**

> Clusters Hyper-V mistos (contendo servidores executando diferentes versões do Hyper-V) não são suportados.

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

- VMs de SO de Desktop ou Servidor compatíveis com a Geração 1.
- VMs de SO de Desktop ou Servidor compatíveis com a Geração 2, incluindo suporte a Inicialização Segura.

Instalar e configurar um hipervisor

> **Importante:**

> Todos os Delivery Controllers devem estar na mesma floresta que os servidores VMM.

1. Instale o servidor Microsoft Hyper-V e o VMM em seus servidores.
2. Instale o console do System Center Virtual Machine Manager em todos os Controllers. A versão do console deve corresponder à versão do servidor de gerenciamento. Embora um console anterior possa se conectar ao servidor de gerenciamento, o provisionamento de VDAs falha se as versões forem diferentes.
3. Verifique as seguintes informações da conta:

A conta que você usa para especificar hosts no Studio é um administrador VMM ou um administrador delegado VMM para as máquinas Hyper-V relevantes. Se esta conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados no Studio durante o processo de criação do host.

> **Dica:**
>
> Ao usar um administrador delegado do VMM, você define um grupo de host de nível superior e concede ao administrador delegado permissões totais apenas para este grupo. Vários grupos de host exigem vários administradores delegados do VMM. Configure um administrador delegado por grupo de host.
>
> A conta de usuário usada para a integração do Studio também deve ser membro do grupo de segurança local de administradores em cada servidor Hyper-V. Essa configuração oferece suporte ao gerenciamento do ciclo de vida da VM, como criação, atualização e exclusão de VMs.

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

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. Crie um snapshot da VM mestre para usar como backup.

Criar desktops virtuais

Se você estiver usando MCS para criar VMs, ao criar um site ou uma conexão:

1. Selecione o tipo de host de virtualização da Microsoft.
2. Insira o endereço como o nome de domínio totalmente qualificado do servidor host.
3. Insira as credenciais para a conta de administrador que você configurou anteriormente que tem permissões para criar VMs.
4. Em **Detalhes do Host**, selecione o cluster ou host autônomo a ser usado ao criar VMs.

   Procure e selecione um cluster ou host autônomo, mesmo que você esteja usando uma implantação de host Hyper-V único.

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 Hipervisor (HCL) do Controller se conectem com sucesso ao armazenamento SMB:

- As credenciais de usuário do VMM devem incluir acesso total de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante eventos do ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Ao usar o armazenamento SMB, habilite o Provedor de Suporte de Segurança de Credencial de Autenticação (CredSSP) do Controller para máquinas Hyper-V individuais. Use este processo para VMM 2012 SP1 com Hyper-V no Windows Server 2012. Para obter mais informações, consulte CTX137465.

A HCL usa `CredSSP` para abrir uma conexão com a máquina Hyper-V. Este 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.

  O HCL carrega a Identidade para a máquina Hyper-V através do compartilhamento do administrador.

  A máquina Hyper-V copia o disco para o armazenamento SMB através de um script PowerShell executado na sessão remota do PowerShell. Uma pasta é criada na máquina Hyper-V e as permissões dessa pasta são bloqueadas apenas para o usuário VMM (através da conexão remota do PowerShell).

  O HCL exclui o arquivo do compartilhamento do administrador.

  Quando o 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, ele o 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 o HCL. O processo a seguir cria uma pasta que tem apenas permissões de usuário VMM no servidor Hyper-V, caso ela não exista.

A máquina Hyper-V copia o disco do armazenamento SMB para o armazenamento Hyper-V local por meio de um script PowerShell. Este script é executado na sessão remota do PowerShell V3.

O HCL lê o disco do compartilhamento do administrador da máquina Hyper-V para a memória.

O HCL exclui o arquivo do compartilhamento do administrador.

Ambientes de virtualização Citrix Hypervisor™

Criar uma conexão com o Citrix Hypervisor

Ao criar uma conexão com o Citrix Hypervisor (anteriormente XenServer®), você deve fornecer as credenciais de um usuário VM Power Admin ou de nível superior.

A Citrix recomenda usar HTTPS para proteger as comunicações com o Citrix Hypervisor. Para usar HTTPS, você deve substituir o certificado SSL padrão instalado no Citrix Hypervisor; consulte CTX128656.

Você pode configurar a alta disponibilidade se ela estiver habilitada no servidor Citrix Hypervisor. A Citrix recomenda que você selecione todos os servidores no pool (em Editar Alta Disponibilidade) para permitir a comunicação com o servidor Citrix Hypervisor caso o mestre do pool falhe.

Você pode selecionar um tipo e grupo de GPU, ou pass-through, se o Citrix Hypervisor suportar vGPU. A exibição indica se a seleção possui recursos de GPU dedicados.

Ao usar armazenamento local em um ou mais hosts Citrix Hypervisor 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 compatíveis.
- UEFI para VMs de SO de desktop ou servidor compatíveis, incluindo Secure Boot.

> **Nota:**
>
> São necessárias permissões de operador de pool ou superiores ao configurar o MCS.

Usar IntelliCache™ para conexões Citrix Hypervisor

Usando o IntelliCache, as implantações 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 Citrix Hypervisor.

- Ao instalar o Citrix Hypervisor, 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 Citrix Hypervisor.
- No Citrix Virtual Apps and Desktops™, o IntelliCache é desabilitado por padrão. Você pode alterar a configuração somente ao criar uma conexão do Citrix Hypervisor; você não pode desabilitar o IntelliCache mais tarde. Ao adicionar uma conexão do Citrix Hypervisor:
  - Selecione **Compartilhado** como o tipo de armazenamento.
  - Marque a caixa de seleção **Usar IntelliCache**.

Permissões necessárias do Citrix Hypervisor

As permissões do Citrix Hypervisor são baseadas em função (RBAC).

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 exigida para cada tarefa de provisionamento.

Criando uma conexão de host

TAREFA	FUNÇÃO MÍNIMA EXIGIDA
Adicionar uma conexão de host usando as informações obtidas do XenServer	Somente leitura
Visualizar usuários e suas funções atribuídas	Somente leitura

Gerenciamento de energia de VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Ligar ou desligar as VMs	Operador de VM

Criar, atualizar ou excluir VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Adicionar ou remover VMs de agendamentos de snapshots existentes	Administrador de energia de VM
Adicionar, modificar, excluir agendamentos de snapshots	Operador de Pool
Publicar imagem mestre	Operador de Pool (Requer bloqueio de porta de switch)
Criar um catálogo de máquinas	Operador de Pool: Requer bloqueio de porta de switch
Adicionar ou remover VMs (VMs não habilitadas para GPU)	Administrador de VM
Adicionar ou remover VMs (VMs habilitadas para GPU)	Operador de Pool
Adicionar, remover ou configurar disco virtual ou dispositivos de CD	Administrador de VM
Gerenciar Tags	Operador de VM

Para obter mais informações sobre funções e permissões RBAC, consulte funções e permissões RBAC.

Para obter informações sobre o bloqueio de porta de switch, consulte Usar bloqueio de porta de switch.

Criar um catálogo de máquinas usando uma conexão Citrix Hypervisor

Máquinas com capacidade de GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure as 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 da GPU (Passthrough ou vGPU).
3. Instale um sistema operacional compatível e habilite o RDP.
4. Instale o Citrix VM Tools e os drivers NVIDIA.
5. Limpe o Console de Administração do Virtual Network Computing (VNC) para otimizar o desempenho e, em seguida, reinicie a VM.
6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e, em seguida, reinicie a VM.
7. Opcionalmente, crie um instantâneo para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente que são configurados no XenCenter e usam recursos de GPU.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

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 ao 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 gerenciar desktops virtuais.

As propriedades booleanas exibidas no Configuration Manager aparecem como `1` ou `0`, não como verdadeiro ou falso.

As propriedades estão disponíveis para a classe `Citrix_virtualDesktopInfo` no namespace `Root\Citrix\DesktopInformation`. Os nomes das propriedades vêm do provedor Windows Management Instrumentation (WMI).

PROPRIEDADE	DESCRIÇÃO
`AssignmentType`	Define o valor de IsAssigned. Os valores válidos são: `ClientIP`, `ClientName`, `None` e `User` (define `IsAssigned` como `True`)
`BrokerSiteName`	Retorna o mesmo valor que `HostIdentifier`
`DesktopCatalogName`	Catálogo de máquinas associado à área de trabalho.
`DesktopGroupName`	Grupo de entrega associado à área de trabalho.
`HostIdentifier`	Retorna o mesmo valor que `BrokerSiteName`.
`IsAssigned`	`True` para atribuir o desktop a um usuário, defina 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

PROPRIEDADE	DESCRIÇÃO
	limpo em uma VM que é provisionada a partir dessa imagem.
`IsVirtualMachine`	`True` para uma máquina virtual, `false` para uma máquina física.
`OSChangesPersist`	`False` se a imagem do sistema operacional 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`	Determinados quando o desktop se registra com o 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 Configuration Manager Resource Explorer. 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 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/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567>`). Quando você desativa esse recurso, o MCS não funciona corretamente.

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

- BIOS herdado para VMs de SO de Desktop ou Servidor compatíveis.
- UEFI para VMs de SO de Desktop ou Servidor compatíveis, incluindo Secure Boot.

Privilégios necessários

Crie uma conta de usuário VMware e uma ou mais funções VMware com um conjunto ou todas as permissões listadas neste artigo. Baseie a criação das funções no nível específico de granularidade exigido sobre as permissões do usuário para solicitar as várias operações do Citrix DaaS™ a qualquer momento. Para conceder as permissões específicas do usuário a qualquer momento, associe-as à função respectiva, no nível do data center, no mínimo, com a opção **Propagate to children** selecionada. No entanto, para as permissões `StorageProfile` e uma permissão `Tags` específica, aplique as permissões no nível do Root vCenter Server, sem **Propagate to Children**. 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 observados nesta página.

Adicionar conexões e recursos

SDK	INTERFACE DO USUÁRIO
System.Anonymous, System.Read e System.View	Adicionado automaticamente. Pode usar a função somente leitura integrada.

Gerenciamento de energia

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interação > Ligar
VirtualMachine.Interact.Reset	Máquina virtual > Interação > Redefinir
VirtualMachine.Interact.Suspend	Máquina virtual > Interação > Suspender
Datastore.Browse	Datastore > Navegar no datastore

Provisionar máquinas (Machine Creation Services)

Para provisionar máquinas usando MCS, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	Datastore > Alocar espaço
Datastore.Browse	Datastore > Navegar no datastore
Datastore.FileManagement	Datastore > Operações de arquivo de baixo nível
Network.Assign	Rede > Atribuir rede
Resource.AssignVMToPool	Recurso > Atribuir máquina virtual ao pool de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuração > Adicionar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuração > Adicionar novo disco
Máquina virtual.Config.Adicionar ou remover dispositivo	Máquina virtual > Configuração > Adicionar ou remover dispositivo
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuração > Avançado

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuração > Remover disco
VirtualMachine.Config.CPUCount	Máquina virtual > Configuração > Alterar contagem de CPU
VirtualMachine.Config.Memory	Máquina virtual > Configuração > Alterar memória
VirtualMachine.Config.Settings	Máquina virtual > Configuração > Alterar configurações
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interação > Ligar
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

SDK	INTERFACE DO USUÁRIO
Datastore.Browse	Datastore > Navegar no datastore
Datastore.FileManagement	Datastore > Operações de arquivo de baixo nível
Network.Assign	Network > Atribuir rede
Resource.AssignVMToPool	Recurso > Atribuir máquina virtual ao pool de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuração > Adicionar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuração > Adicionar novo disco
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

SDK	INTERFACE DO USUÁRIO
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 armazenamento de dados 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 Root vCenter Server, sem **Propagar para Filhos**.

Tags e Atributos Personalizados

Tags e atributos personalizados permitem anexar metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e filtragem desses objetos. Para criar, editar, atribuir e excluir tags ou categorias, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
InventoryService.Tagging.CreateTag	Marcação vSphere > Criar Marcação vSphere
InventoryService.Tagging.CreateCategory	Marcação vSphere > Criar Categoria de Marcação vSphere
InventoryService.Tagging.EditTag	Marcação vSphere > Editar Marcação vSphere
InventoryService.Tagging.EditCategory	Marcação vSphere > Editar Categoria de Marcação vSphere
InventoryService.Tagging.DeleteTag	Marcação vSphere > Excluir Marcação vSphere
InventoryService.Tagging.DeleteCategory	Marcação vSphere > Excluir Categoria de Marcação vSphere
InventoryService.Tagging.AttachTag	Marcação vSphere > Atribuir ou Desatribuir Marcação vSphere
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Atribuir ou Desatribuir Tag vSphere em Objeto
Global.ManageCustomFields	Global > Gerenciar atributos personalizados
Global.SetCustomField	Global > Definir atributo personalizado

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:

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 as seguintes.

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.AddRemoveDevice	Máquina virtual > Configuração > Adicionar ou remover dispositivo
VirtualMachine.Config.CPUCount	Máquina virtual > Configuração > Alterar contagem de CPU
VirtualMachine.Config.Memory	Máquina virtual > Configuração > Memória
VirtualMachine.Config.Settings	Máquina virtual > Configuração > Configurações
VirtualMachine.Provisioning.CloneTemplate	Máquina virtual > Provisionamento > Clonar modelo
VirtualMachine.Provisioning.DeployTemplate	Máquina virtual > Provisionamento > Implantar modelo
VApp.Export	vApp > Export

Observação:

O `VApp.Export` é necessário para criar catálogos de máquinas MCS usando 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.

O HTTPS requer certificados digitais. Use um certificado digital emitido por uma autoridade de certificação que atenda à política de segurança da sua organização.

Se você não conseguir usar um certificado digital emitido por uma autoridade de certificação, você pode usar o certificado autoassinado instalado pelo VMware. Use este método somente 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 somente se o FQDN do computador que executa o vCenter Server ainda não estiver presente no sistema de nomes de domínio.

2. Obtenha o certificado 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.

   Importar diretamente do Internet Explorer executado como administrador.

   - Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com)>`.
   - Aceite os avisos de segurança.
   - Clique na barra de endereço que exibe o erro de certificado.
   - Visualize o certificado.

3. Importe o certificado para o armazenamento de certificados em cada um dos seus Controladores.

   a. Clique na opção **Instalar certificado**, selecione **Máquina Local** e, em seguida, clique em **Avançar**.

b. Selecione **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.

Considerações de configuração

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.

Criar uma conexão:

No assistente de criação de conexão:

- Selecione o tipo de conexão VMware.
- Especifique o endereço do ponto de acesso para o SDK do vCenter.
- 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.

Solução de problemas

Se a criação do catálogo falhar, consulte CTX294978.

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.

Configurando o cluster AVS

Para permitir que o Citrix Virtual Apps™ and Desktop Service use o AVS, execute as seguintes etapas no Azure:

- Solicitar uma cota de host
- Registrar o provedor de recursos Microsoft.AVS
- Lista de Verificação de Rede
- Criar uma nuvem privada do Azure VMware Solution
- Acessar uma nuvem privada do Azure VMware Solution
- Configurar a rede para sua nuvem privada VMware no Azure
- Configurar DHCP para Azure VMware Solution
- Adicionar um segmento de rede no Azure VMware Solution
- Verificar o ambiente do Azure VMware Solution

SOLICITAR COTA DE HOST PARA CLIENTES DO CONTRATO ENTERPRISE DO AZURE

Na página **Ajuda + Suporte** do portal do Azure, selecione **Nova solicitação de suporte** e inclua as seguintes informações:

- Tipo de problema: Técnico
- Assinatura: Selecione sua assinatura
- Serviço: Todos os serviços > Solução VMware do Azure
- 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

> **Observação:**
>
> O AVS requer um mínimo de três hosts e recomenda que você use redundância de hosts N+1.

> Após especificar os detalhes para o tíquete de suporte, selecione **Revisar + Criar** para enviar a solicitação ao Azure.

REGISTRAR O PROVEDOR DE RECURSOS MICROSOFT.AVS

Após solicitar a cota de host, registre o provedor de recursos:

1. Faça login no portal do Azure.
2. No menu do portal do Azure, selecione **Todos os serviços**.
3. No menu **Todos os serviços**, insira a assinatura e selecione **Assinaturas**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Provedores de recursos** e insira **Microsoft.AVS** na barra de pesquisa.

6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

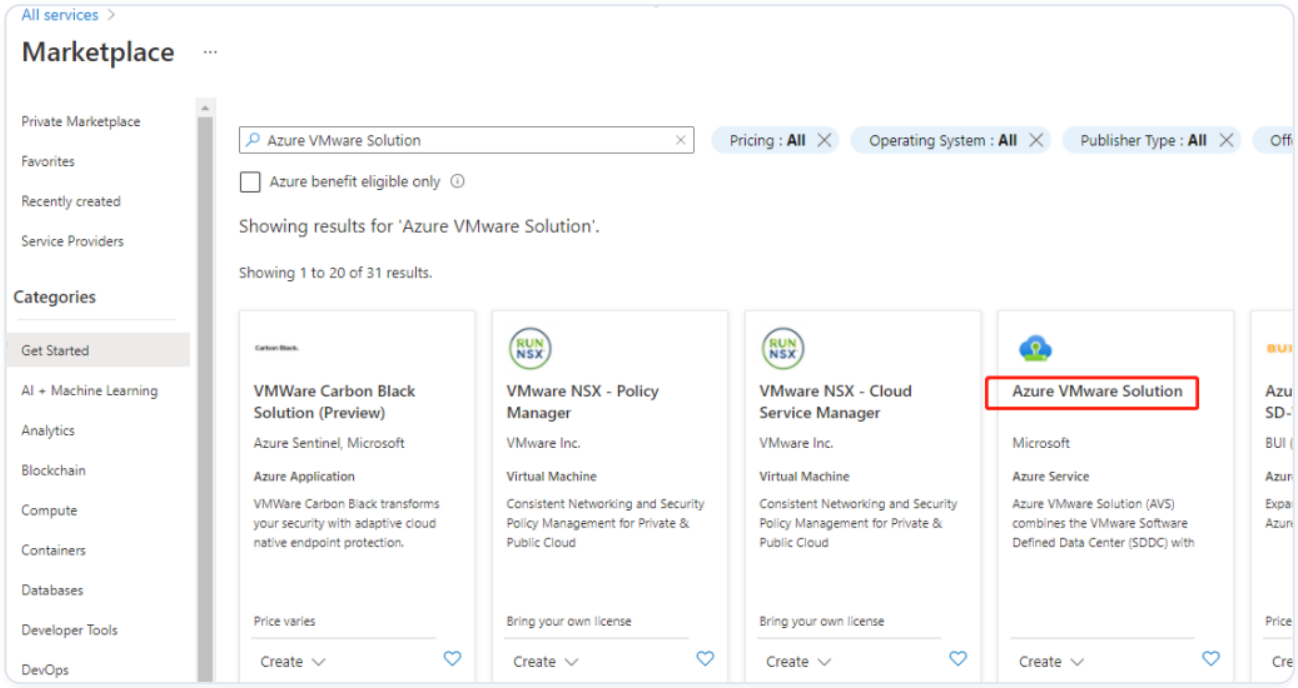
CONSIDERAÇÕES SOBRE REDE

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

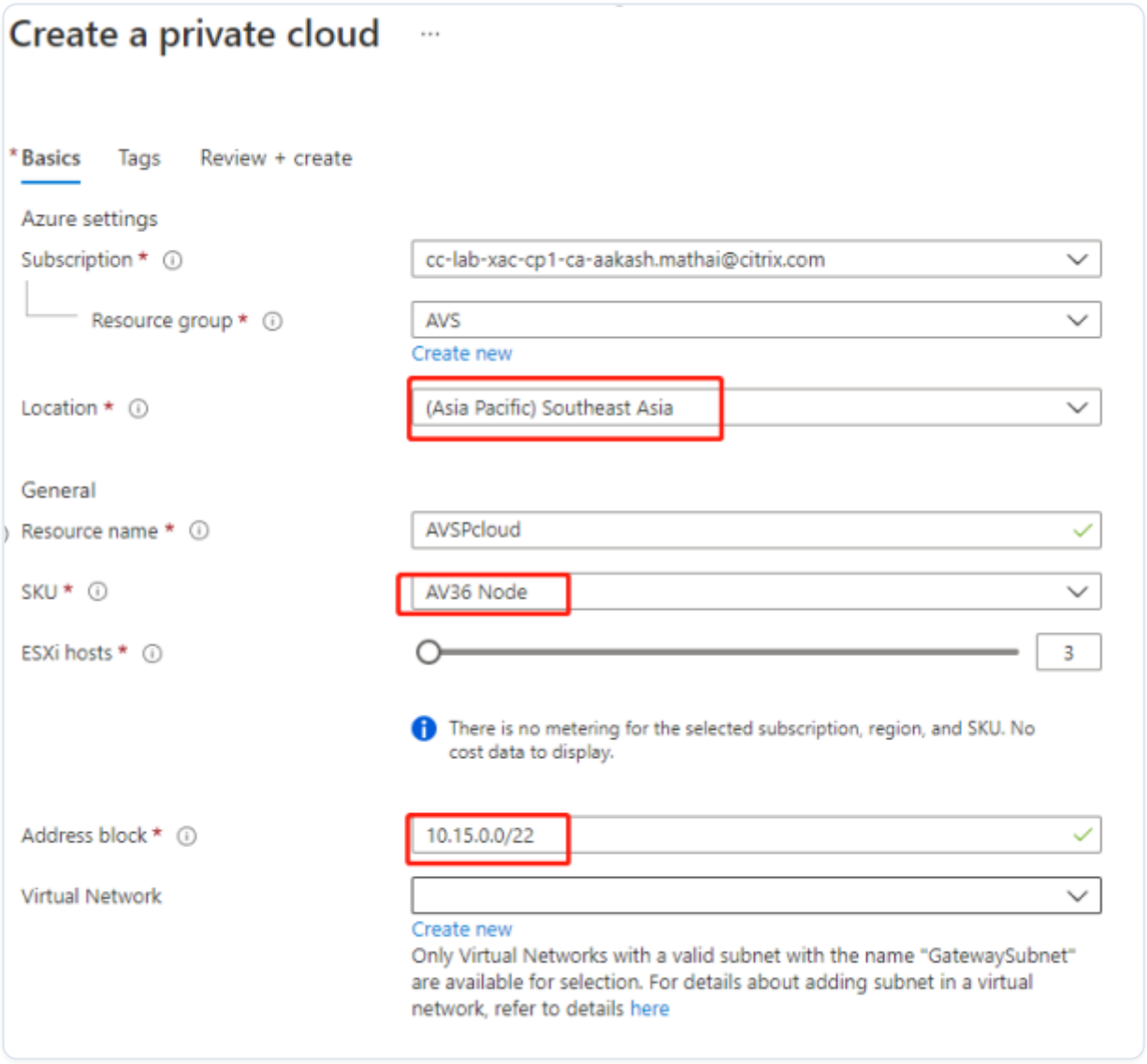
Na janela **Azure VMware Solution**:

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.
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 da Solução VMware do Azure.
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 endereço	Forneça um bloco de endereço IP para a nuvem privada. O CIDR representa a rede de gerenciamento da nuvem privada e será usado para os serviços de gerenciamento de cluster, como vCenter Server e NSX-T Manager. Use o espaço de endereço /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure, bem como a redes locais.
Rede Virtual	Deixe este campo em branco porque o circuito ExpressRoute do Azure VMware Solution é estabelecido como uma etapa pós-implantação.

Na tela **Criar uma nuvem privada**:

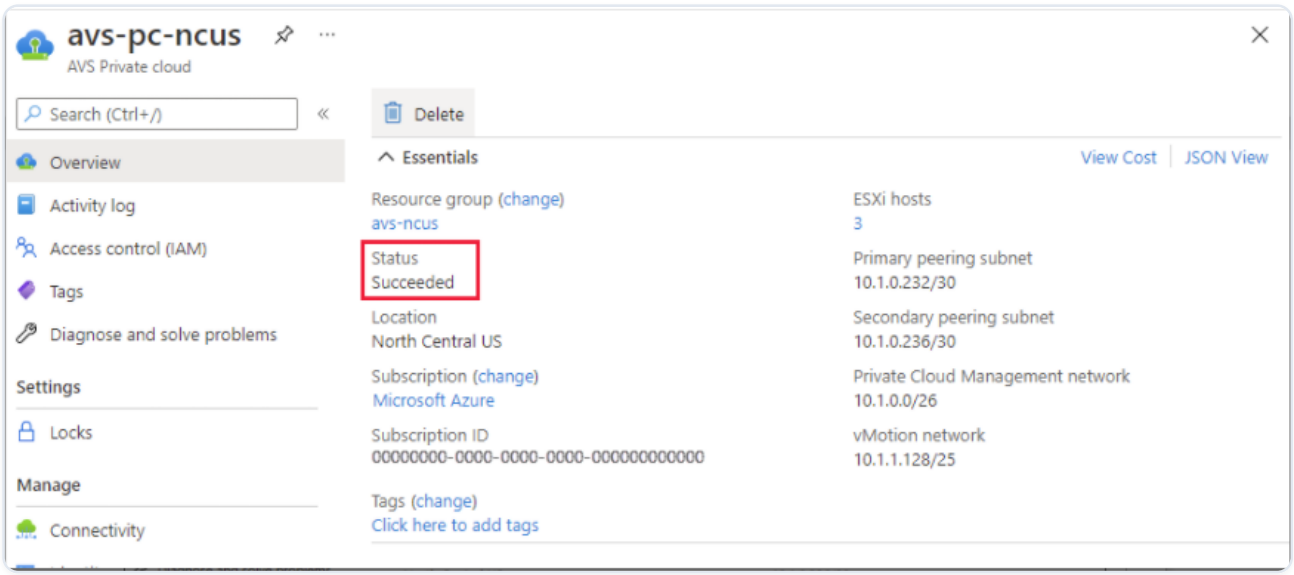
1. No campo **Localização**, selecione a região que possui o AVS; a região do grupo de recursos é a mesma da região do AVS.
2. No campo **SKU**, selecione **AV36 Node**.
3. Especifique um endereço IP no campo **Address Block**. Por exemplo, 10.15.0.0/22.
4. Selecione **Revisar + Criar**.
5. Após revisar as informações, clique em **Criar**.



Dica:

A criação de uma nuvem privada pode levar de 3 a 4 horas. Adicionar um único host ao cluster pode levar de 30 a 45 minutos.

> Verifique se a implantação foi bem-sucedida. navegar até o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Succeeded**, a implantação estará concluída.



ACESSAR UMA NUVEM PRIVADA DO AZURE VMWARE SOLUTION

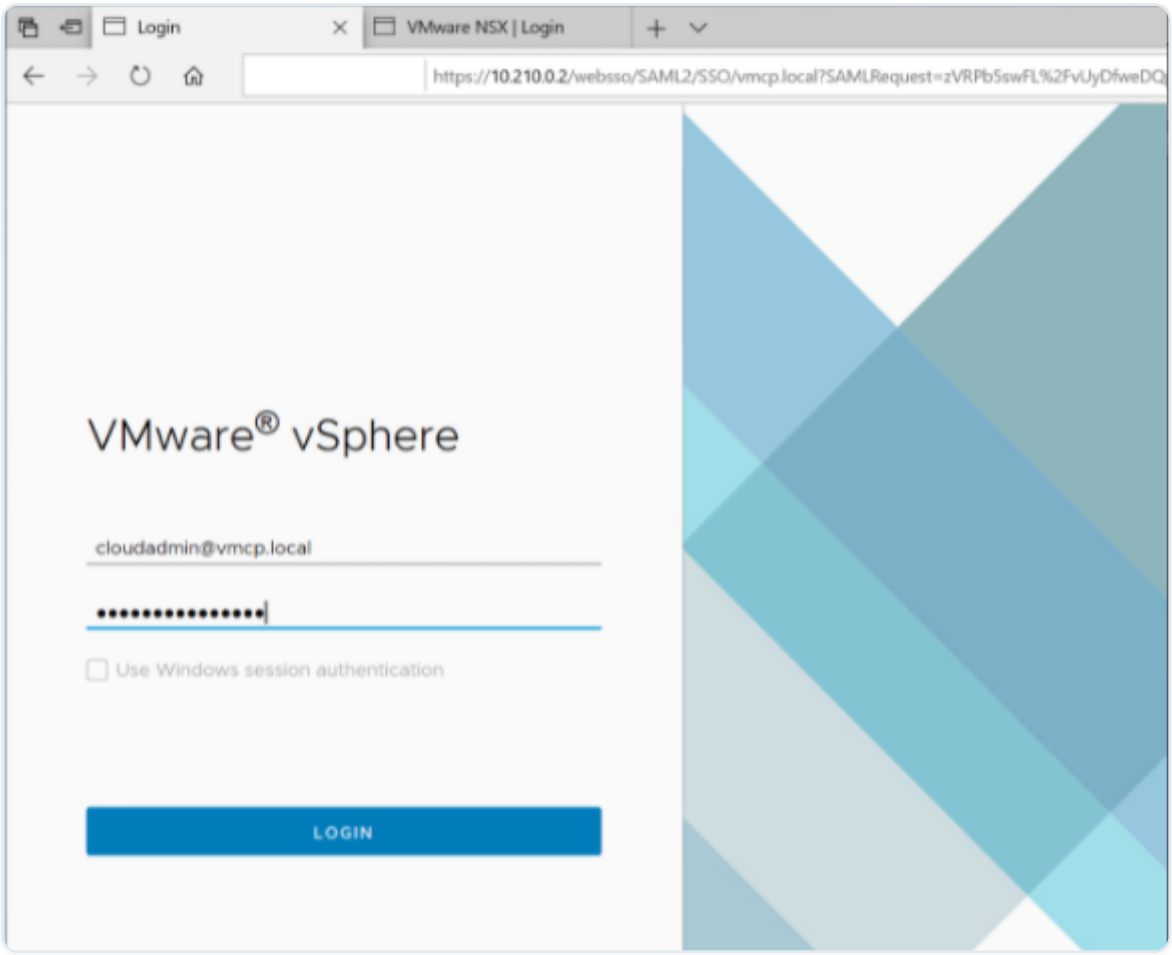
Depois de criar uma nuvem privada, crie uma VM do Windows e conecte-se ao vCenter local da sua nuvem privada.

Criar uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar**, depois 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.

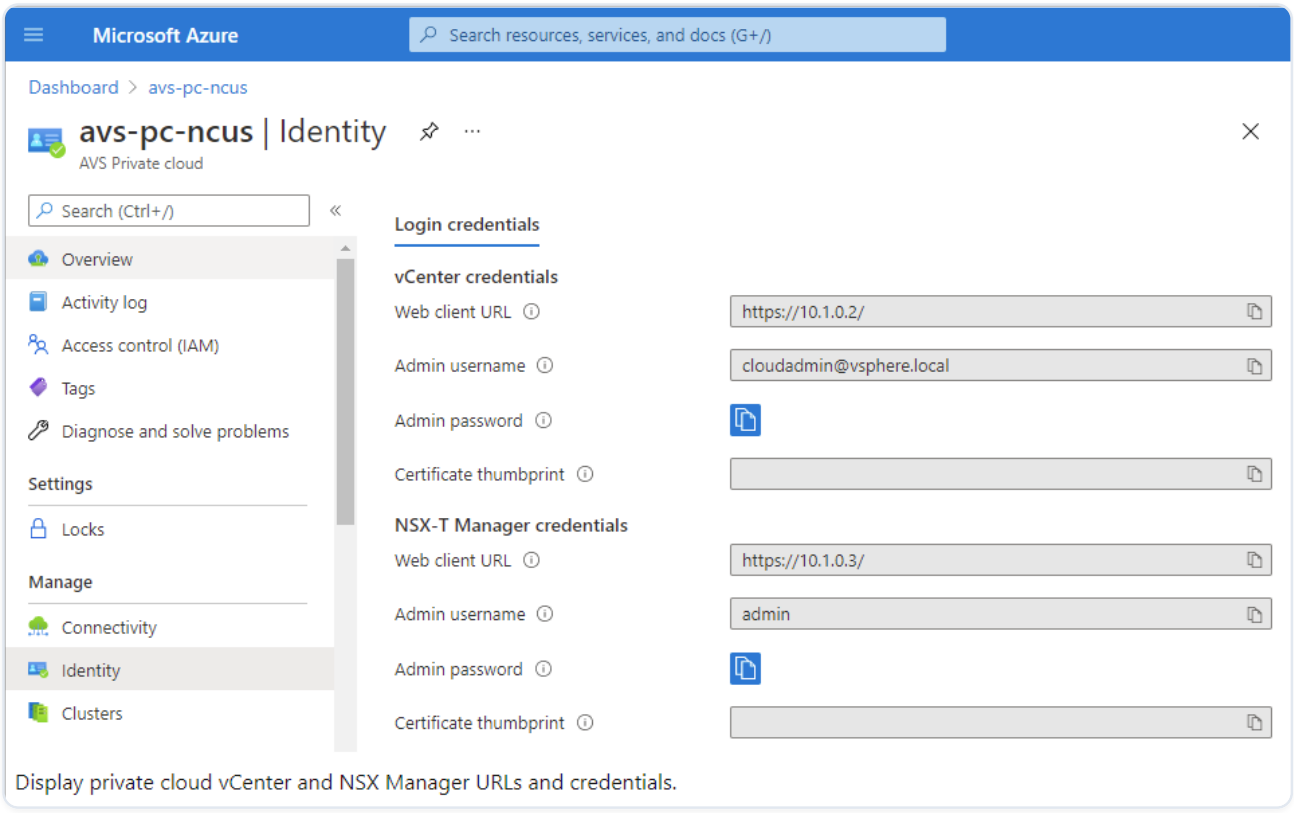
Conectar-se ao vCenter local da sua nuvem privada

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 até a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegar para as URLs do vCenter e do NSX-T Manager em duas guias do navegador. Na guia do vCenter, insira as credenciais de usuário *cloudadmin@vmcp.local* da etapa anterior.

CONFIGURAR A REDE PARA SUA NUVEM PRIVADA VMWARE NO AZURE

Após acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.
Criar uma rede virtual

1. Faça login no portal do Azure.
2. navegar para o grupo de recursos criado anteriormente.
3. Selecione **+ Adicionar** para definir um novo recurso.
4. Na caixa de texto **Pesquisar no Marketplace**, digite *rede virtual*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Rede Virtual**, selecione **Criar** para configurar a rede virtual para sua nuvem privada.
6. Na página **Criar Rede Virtual**, insira os detalhes da sua rede virtual.
7. Na guia **Básico**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Avançar: Endereços IP.**

8. Na guia **Endereços IP**, em espaço de endereço IPv4, insira o endereço criado anteriormente.

> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço que você usou ao criar sua nuvem privada.

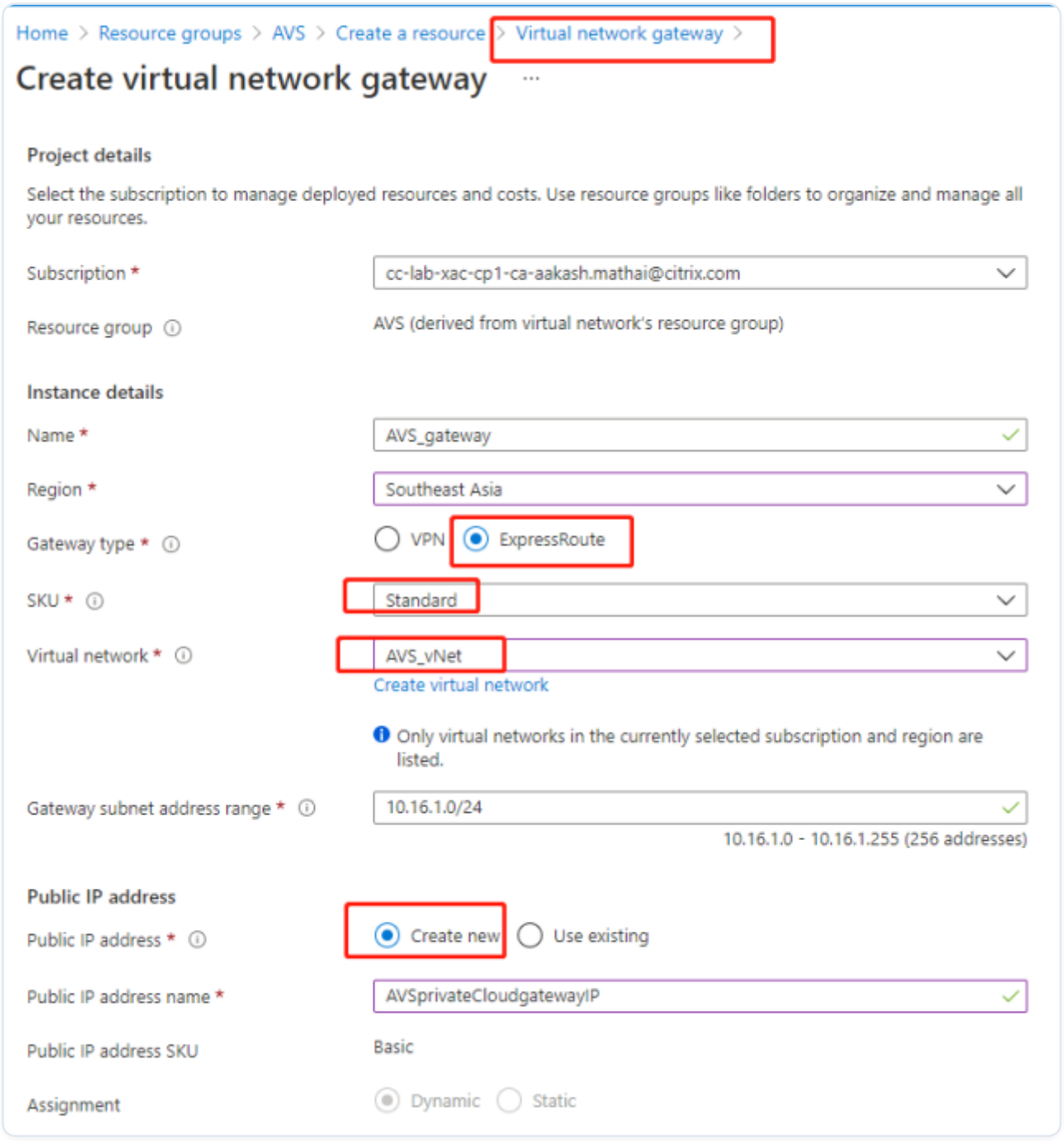
> Após inserir o espaço de endereço:

1. Selecione **+ Adicionar sub-rede**.
2. Na página **Adicionar sub-rede**, dê um nome à sub-rede e um intervalo de endereços apropriado.
3. Clique em **Adicionar.**
4. Selecione **Revisar + criar**.
5. Verifique as informações e clique em **Criar**. Assim que a implantação for concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual

Após criar uma rede virtual, crie um gateway de rede virtual.

1. No seu grupo de recursos, selecione **+ Adicionar** para adicionar um novo recurso.
2. Na caixa de texto **Pesquisar no Marketplace**, digite *gateway de rede virtual*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Gateway de Rede Virtual**, clique em **Criar**.
4. Na guia **Básico** da página **Criar gateway de rede virtual**, forneça valores para os campos.
5. Clique em **Revisar + criar**.



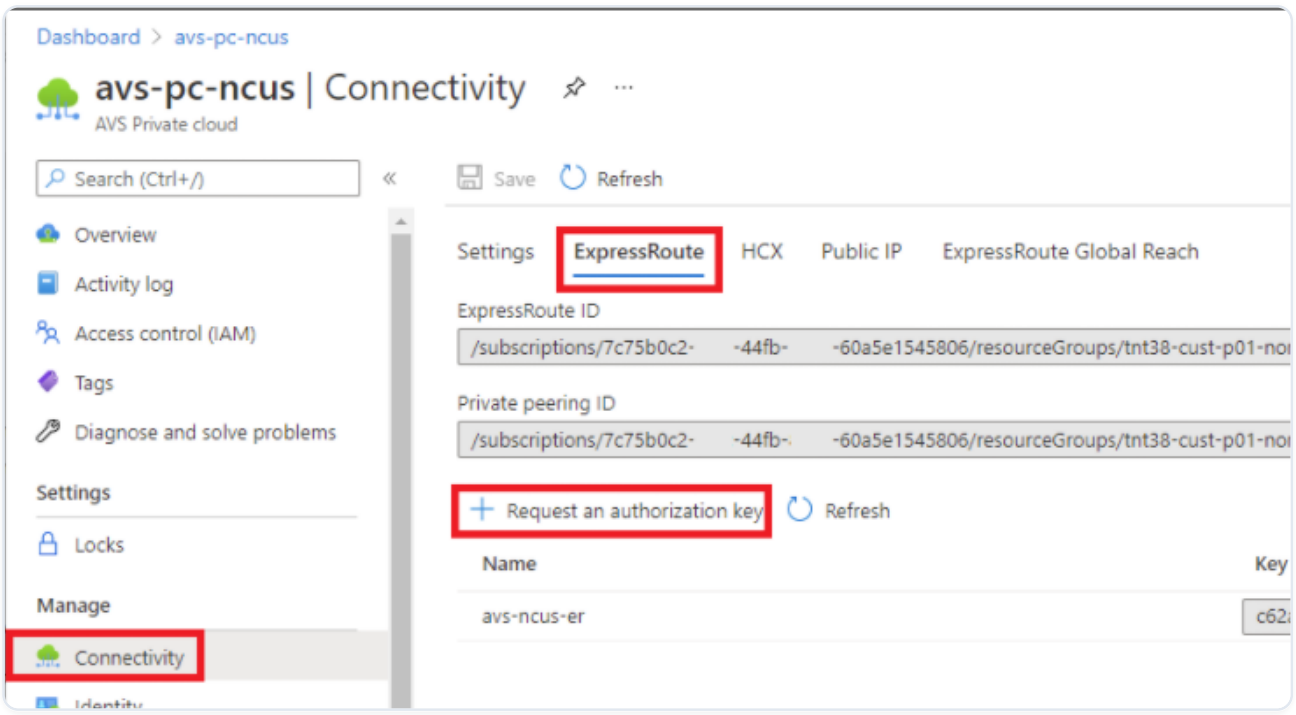
Após revisar a configuração do gateway de rede virtual, clique em **Criar** para implantar seu gateway de rede virtual. Assim que a implantação for concluída, conecte sua conexão **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada Azure AVS.

CONECTAR O EXPRESSROUTE AO GATEWAY DE REDE VIRTUAL

Após implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada Azure AVS:

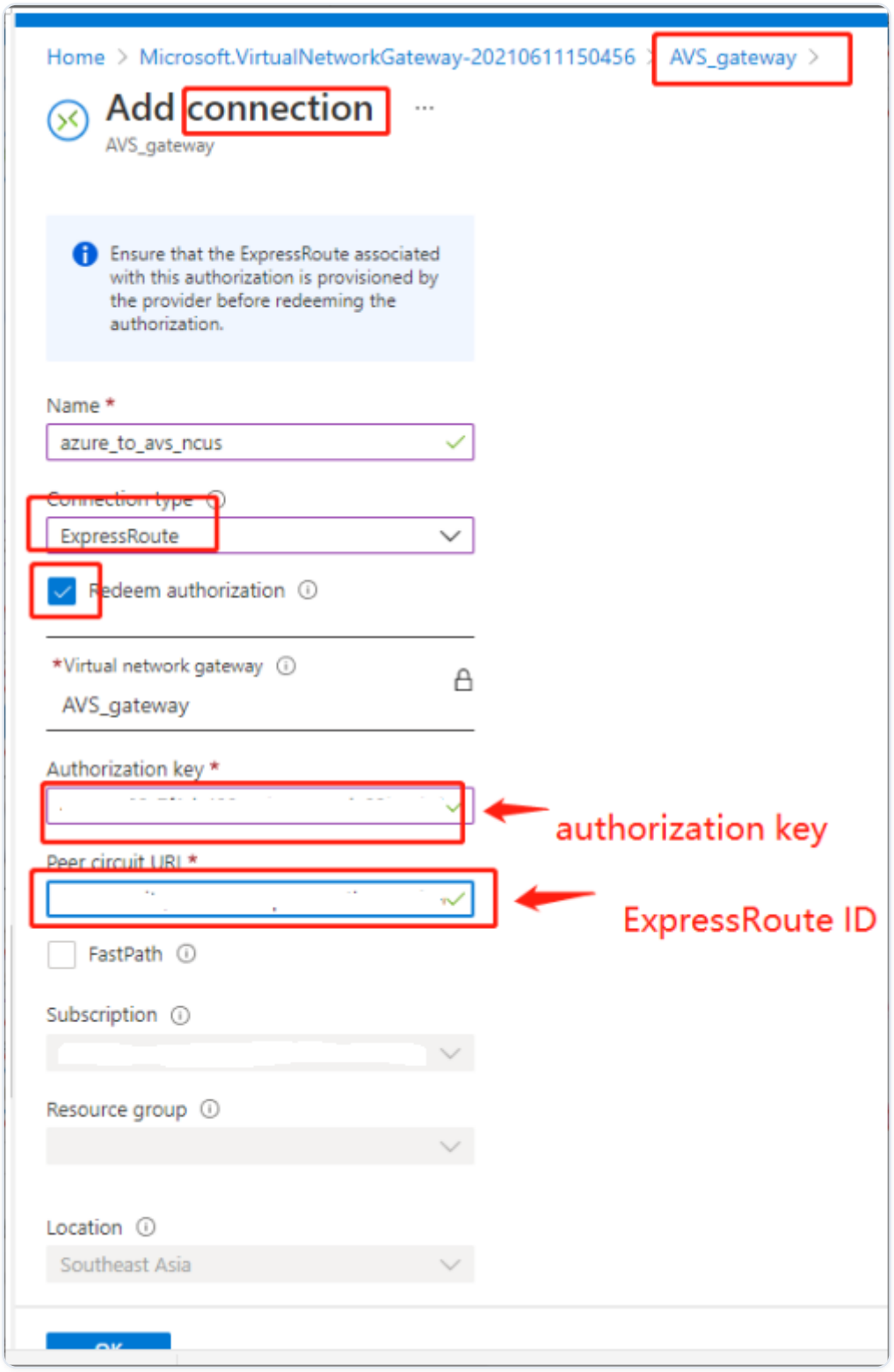
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegar até a **nuvem privada da Solução VMware do Azure**. Selecione **Gerenciar > Conectividade > ExpressRoute** e, em seguida, selecione **+ Solicitar uma chave de autorização.**

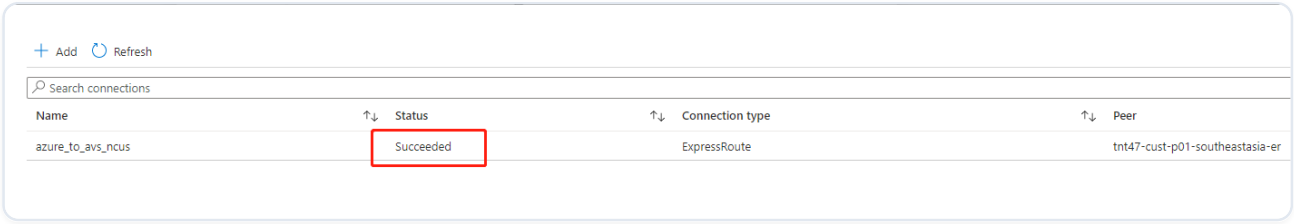


Após solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Criar**. Pode levar cerca de 30 segundos para criar a chave. Uma vez criada, a nova chave aparece na lista de chaves de autorização para a nuvem privada.
2. Copie a **chave de autorização** e o **ID do ExpressRoute**. Você precisará deles para concluir o processo de emparelhamento. A chave de autorização desaparece 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:



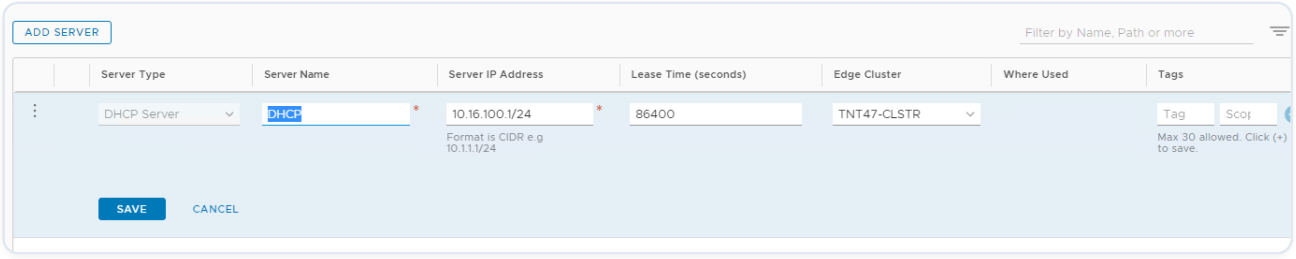
CONFIGURAR DHCP PARA AZURE VMWARE SOLUTION

Após conectar o ExpressRoute ao gateway virtual, configure o DHCP.

Use o NSX-T para hospedar seu servidor DHCP

No NSX-T Manager:

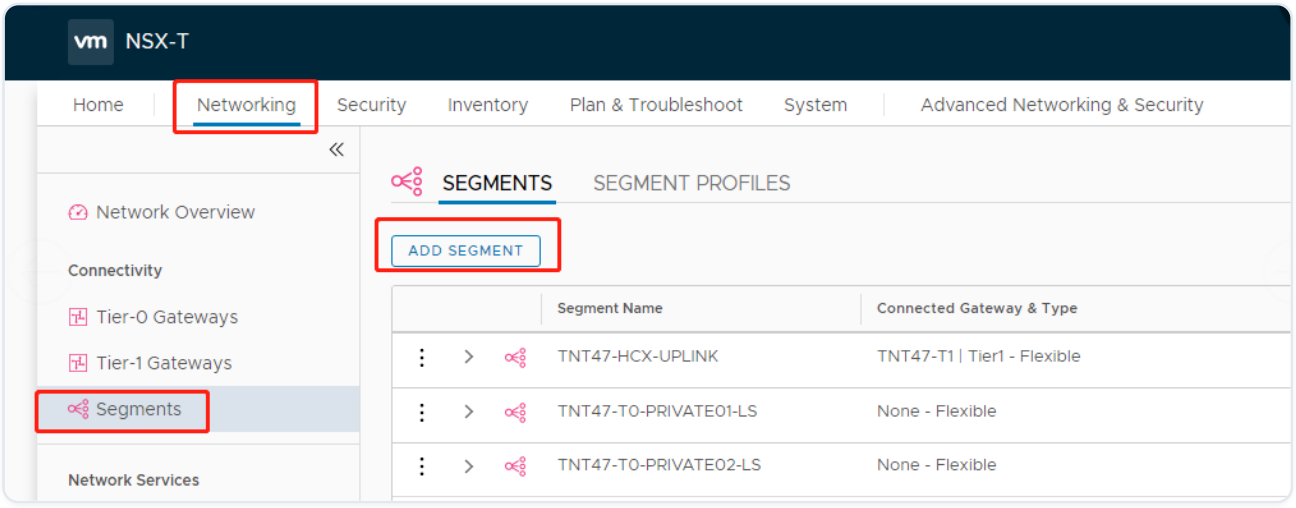
1. Selecione **Rede > DHCP** e então selecione **Adicionar Servidor**.
2. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Gateways de Camada 1**, selecione as reticências verticais no gateway de Camada 1 e então selecione **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

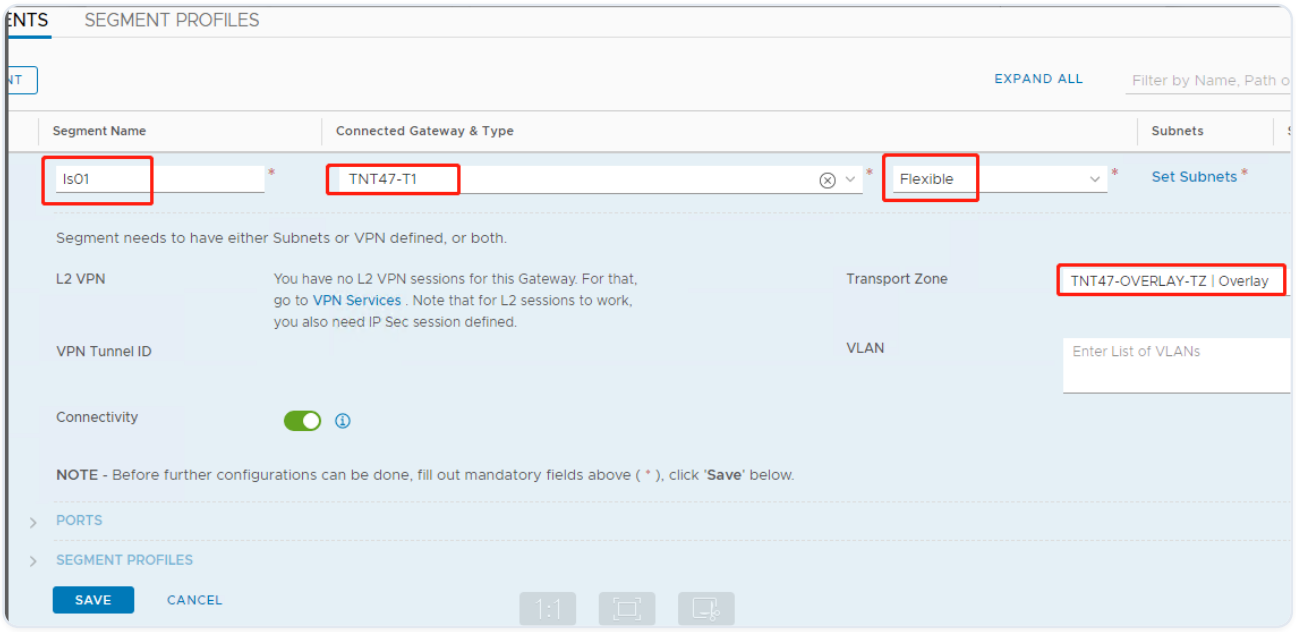
Após configurar o DHCP, adicione um segmento de rede.

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**:

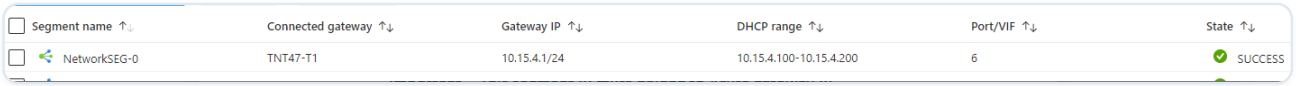
1. Insira um **nome** para o segmento.
2. Selecione o **Gateway Tier-1 (TNTxx-T1)** como o **Gateway Conectado** e deixe o **Tipo** como **Flexível**.
3. Selecione a **Zona de Transporte (TNTxx-OVERLAY-TZ)** de sobreposição pré-configurada.
4. Clique em **Definir Sub-redes**.



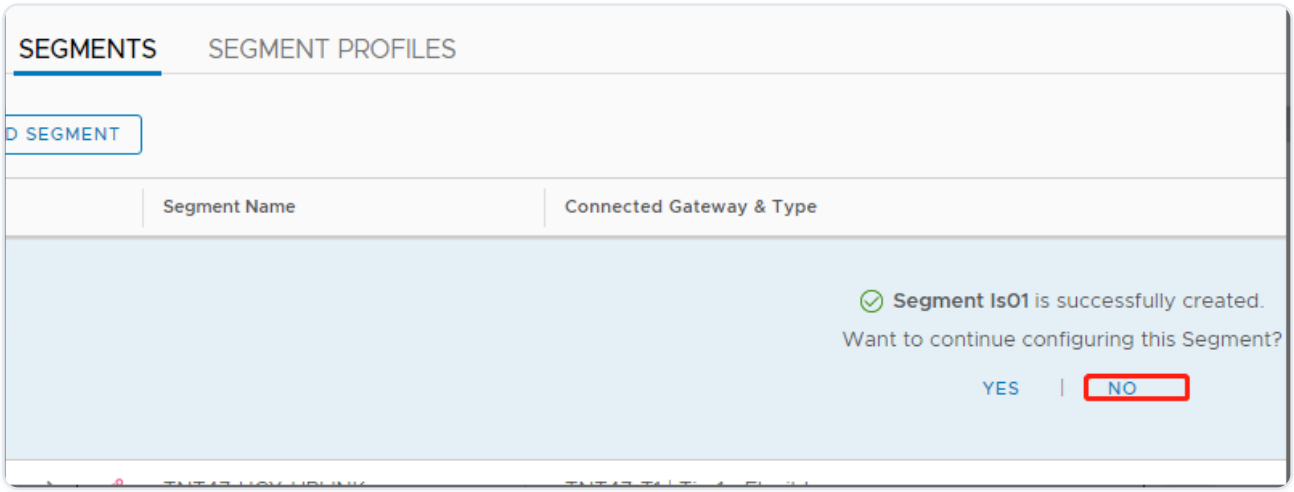
Na seção **Sub-redes**:

1. Insira o endereço IP do gateway.
2. Selecione **Adicionar**.

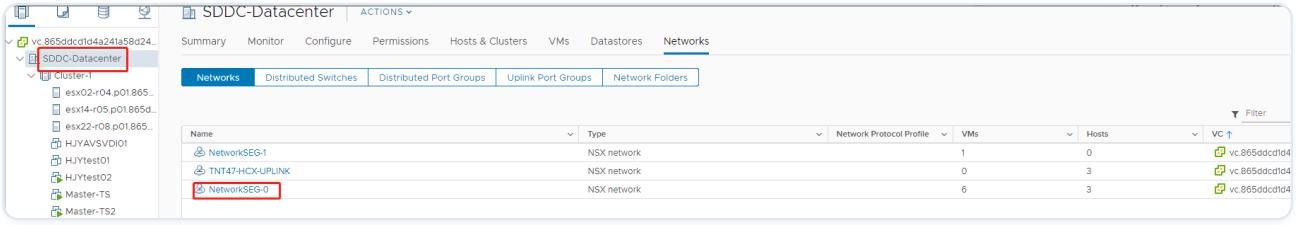
> **Importante:**
>
> Este endereço IP de segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.
>
> O intervalo DHCP deve pertencer ao endereço IP do segmento:



Selecione **Não** para recusar a opção de continuar configurando o segmento:

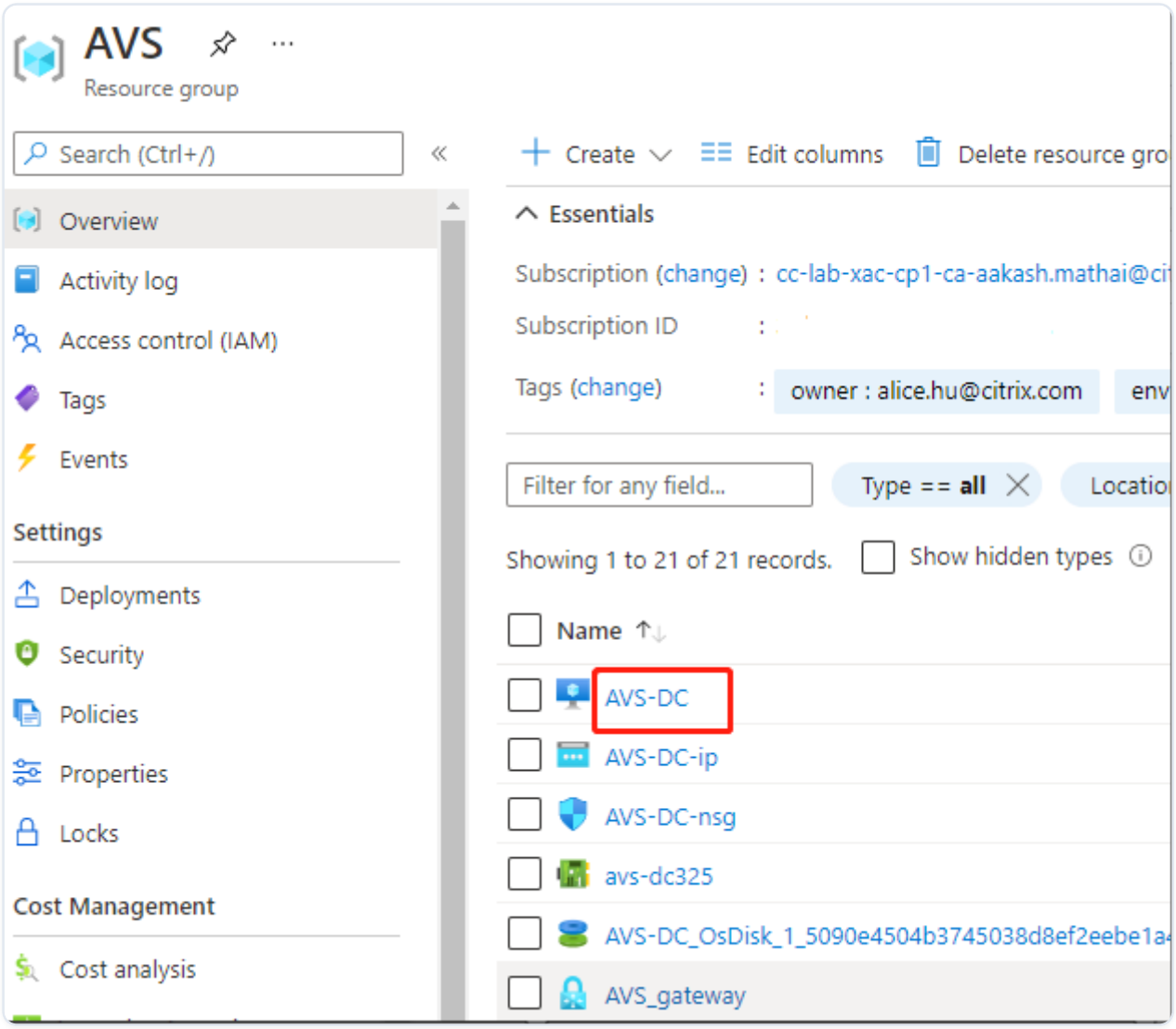


No vCenter, selecione **Networking > SDDC-Datacenter**:

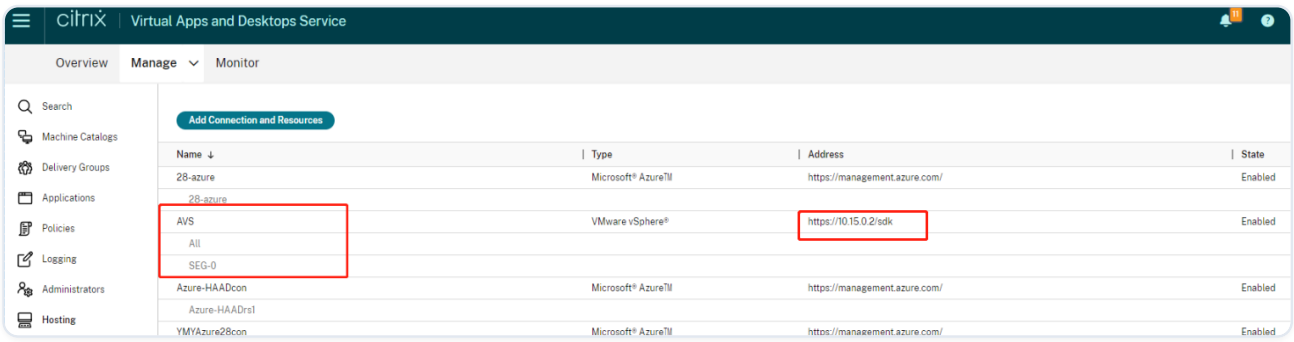


VERIFICAR O AMBIENTE AZURE AVS

Configurar uma conexão direta e um conector no grupo de recursos do Azure:



Verificar 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.

Configurando 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 de Camada 1**, selecione as reticências verticais no gateway de Camada 1 e então 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

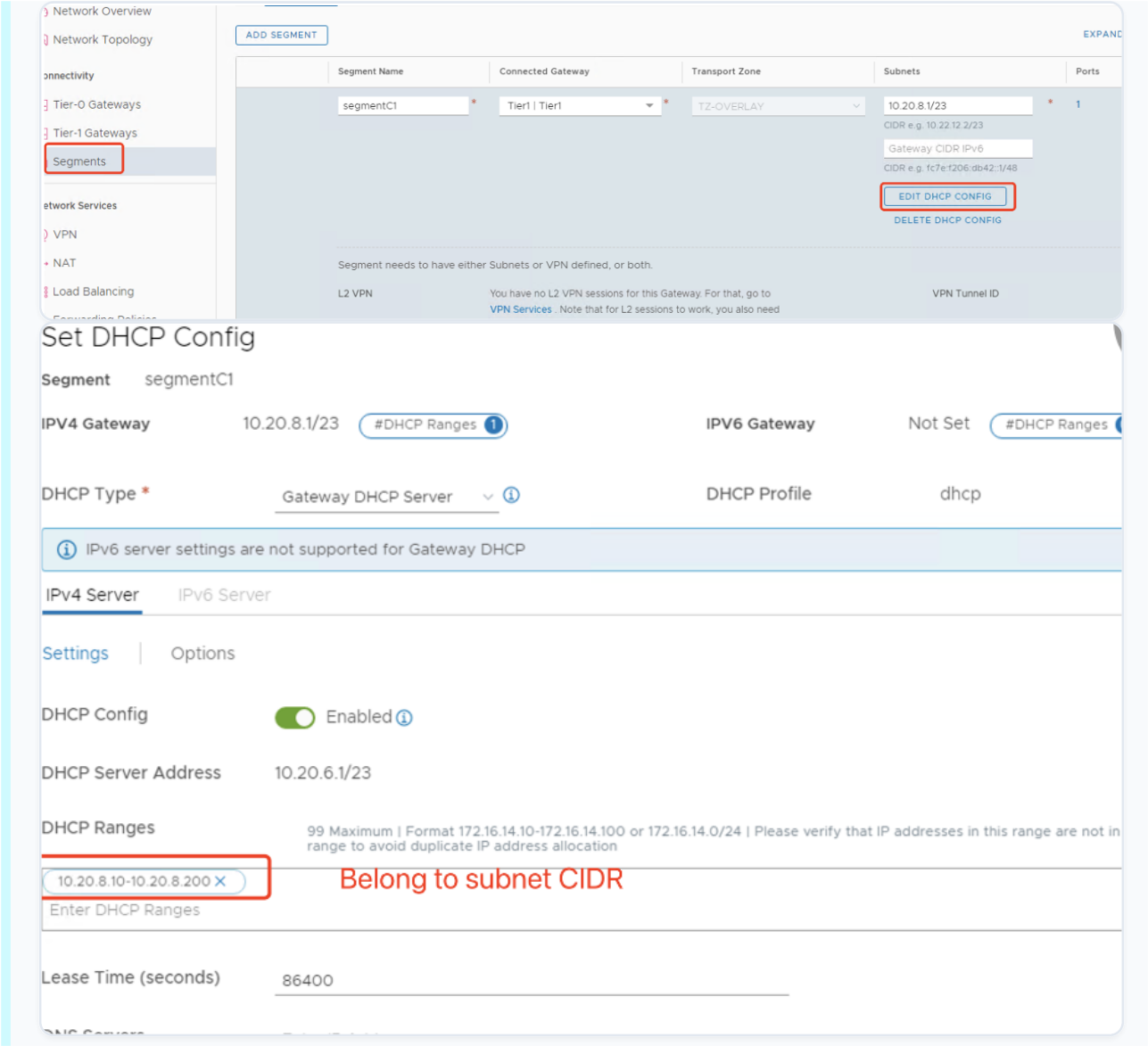
Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede NSX-T para sua nuvem privada:

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.

> **Observação:**
>
> 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:

   Adicionar Conexão e Recursos(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/gcp-vmware-add-connection.png)

   a. Selecione **Tipo de conexão** como **VMware vSphere**.
   b. Em **Endereço de conexão**, insira o endereço IP privado do vCenter.
   c. Insira as credenciais do vCenter.
   d. Insira um nome de conexão.

e. Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Rede**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

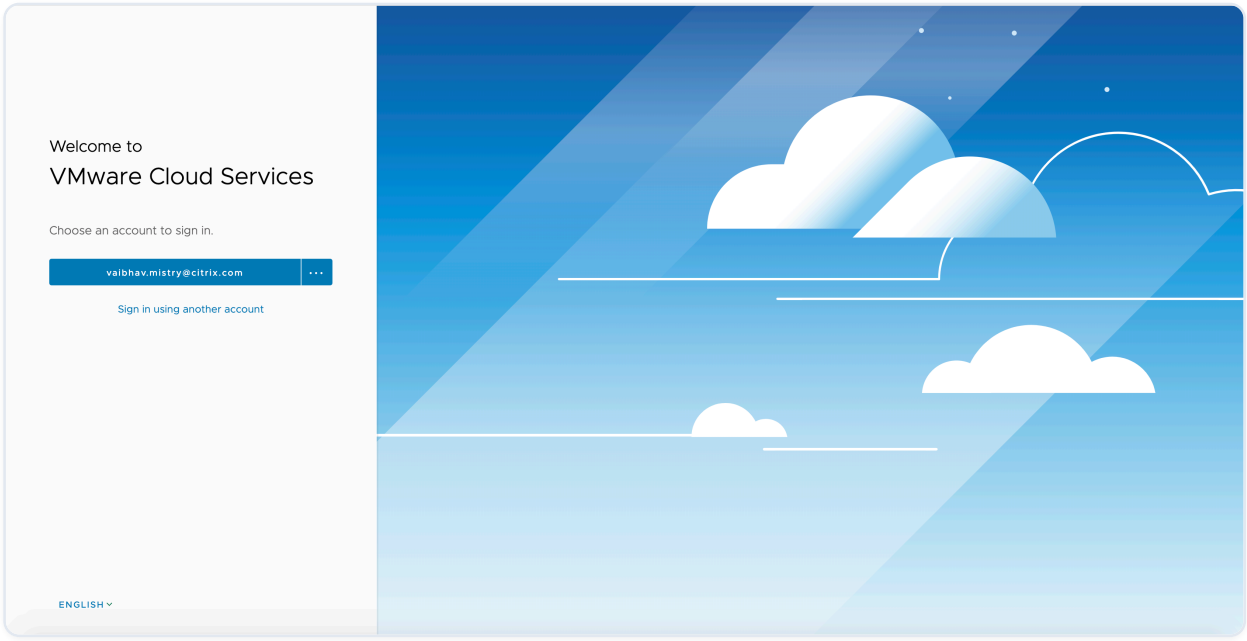
VMware Cloud no Amazon Web Services (AWS)

O VMware Cloud no Amazon Web Services (AWS) permite migrar cargas de trabalho Citrix locais baseadas em VMware para a nuvem AWS.

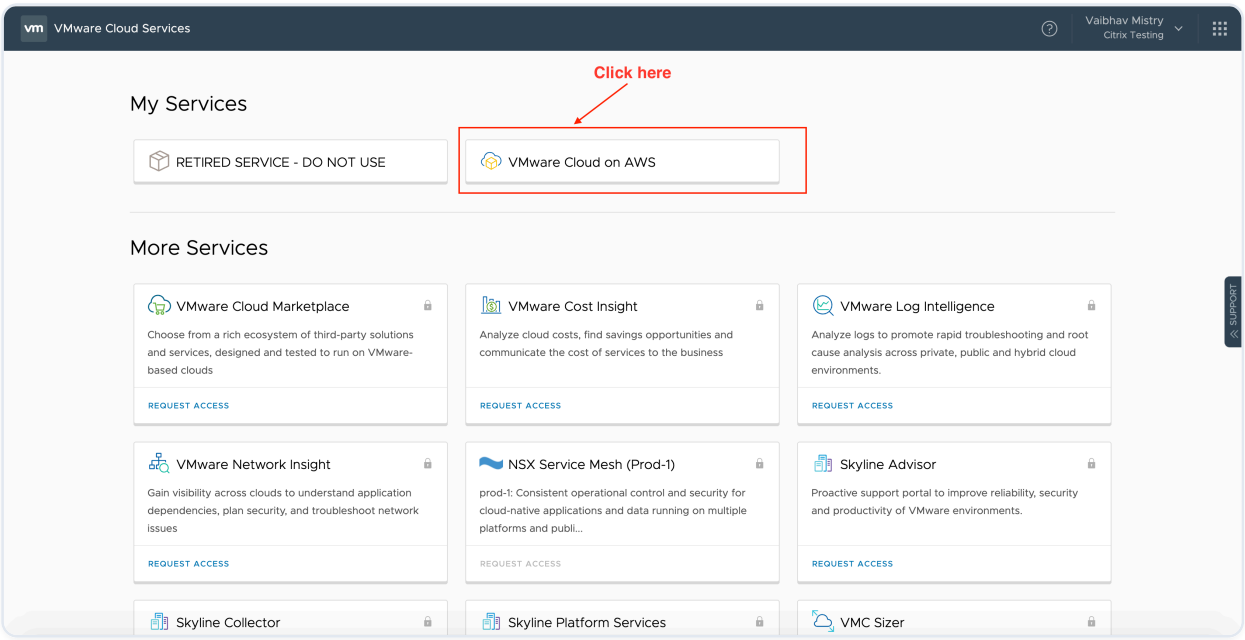
Este artigo descreve o procedimento para configurar um VMware Cloud no AWS.

Acessar o ambiente VMware Cloud

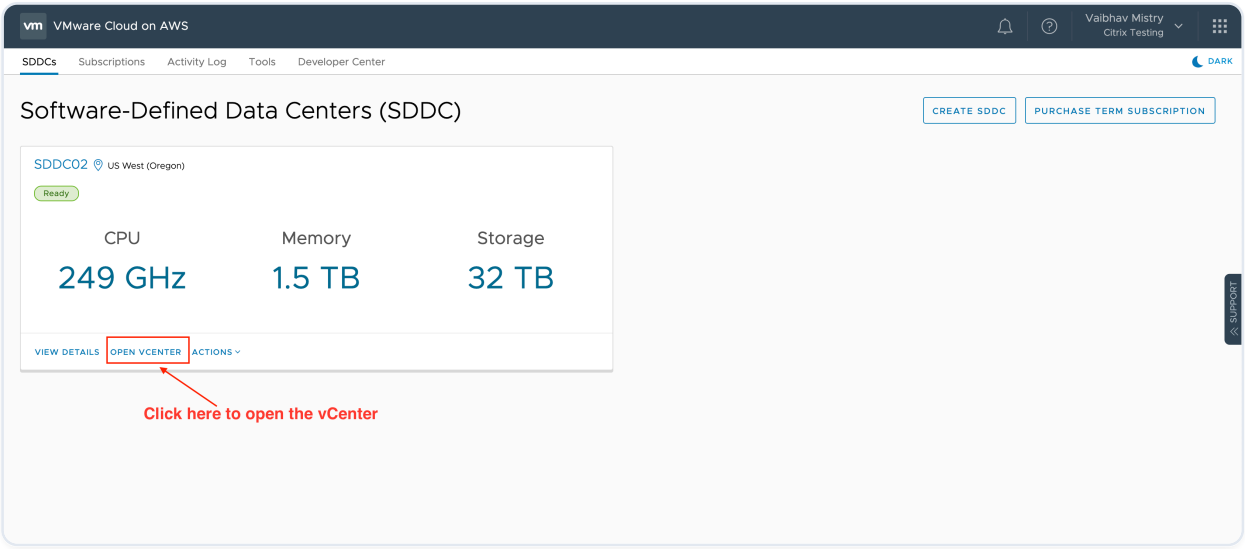
1. Faça login nos serviços de nuvem VMware usando o URL `<https://console.cloud.vmware.com/>`.

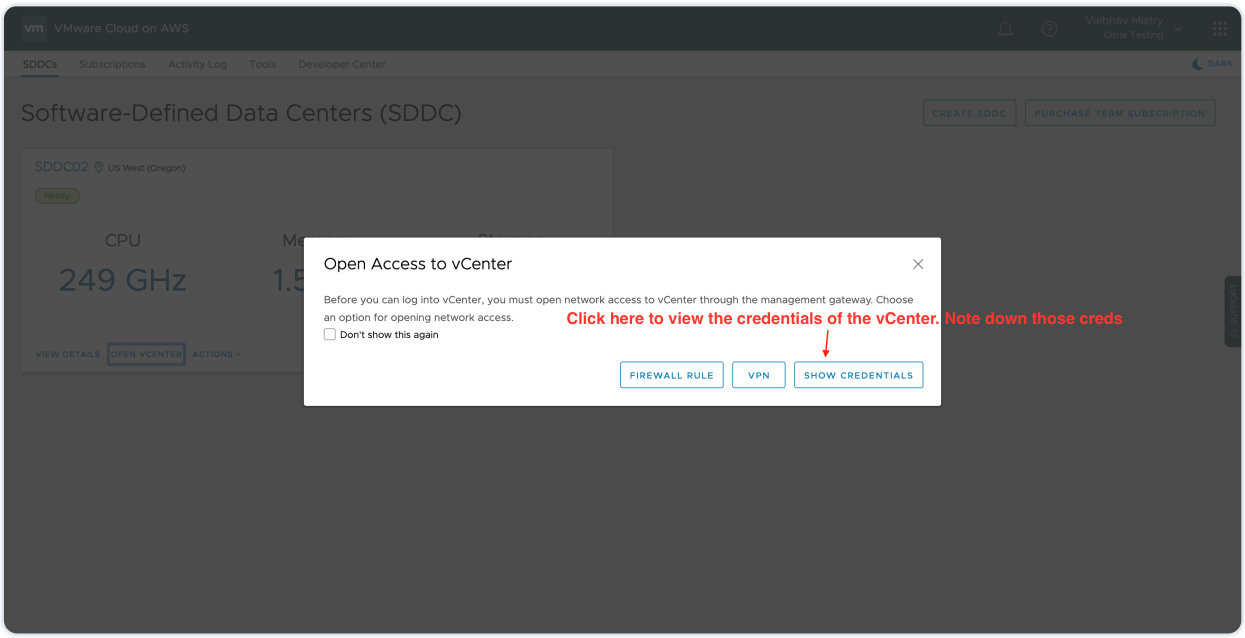


2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

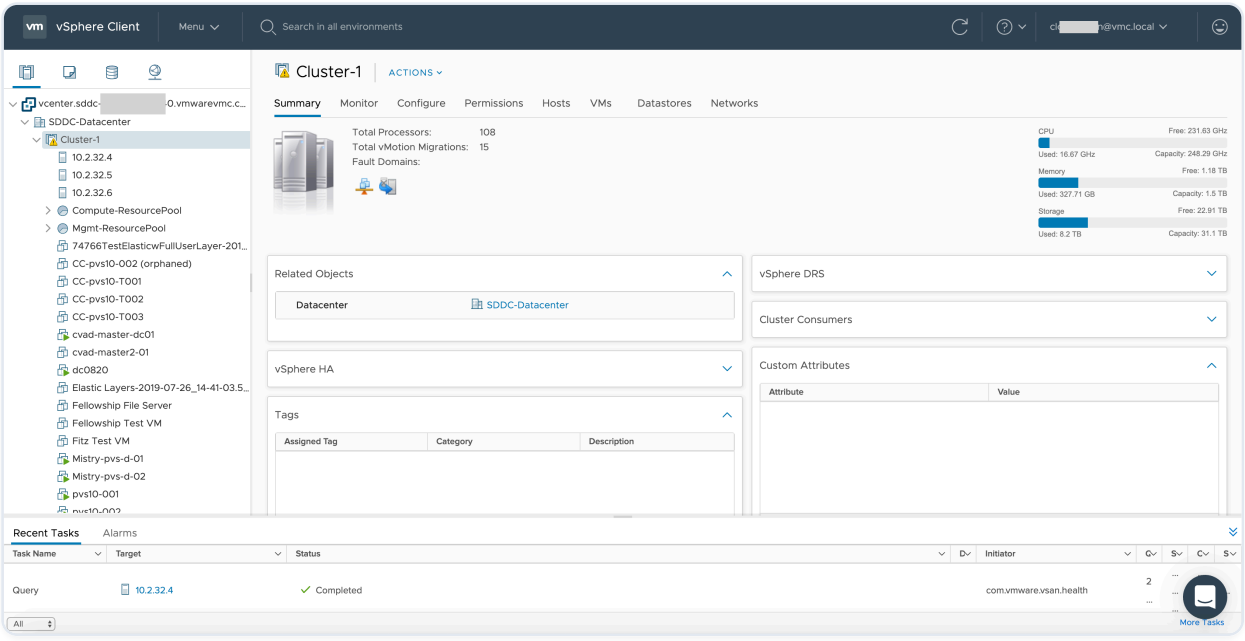


3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Anote as credenciais para uso posterior.





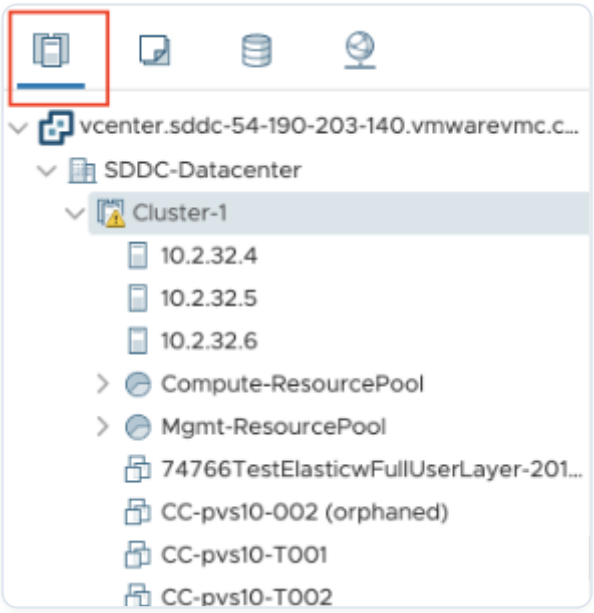
4. Abra um navegador da Web e insira o URL do vSphere Web Client.
5. Insira as credenciais conforme observado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



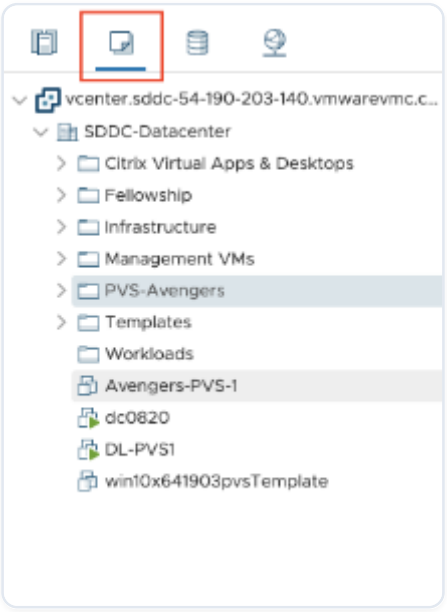
Sobre o ambiente de nuvem VMware

Existem quatro visualizações na página da Web do cliente vSphere.

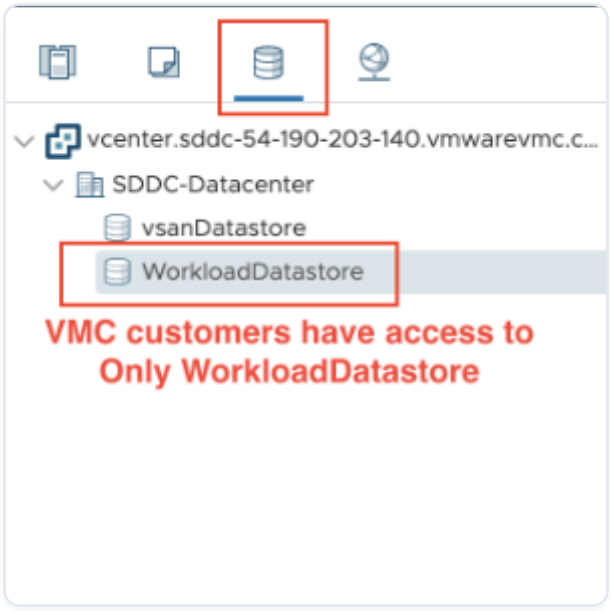
- Visualização de Host e Cluster: Você não pode criar um novo Cluster, mas o administrador da nuvem pode criar vários pools de recursos.



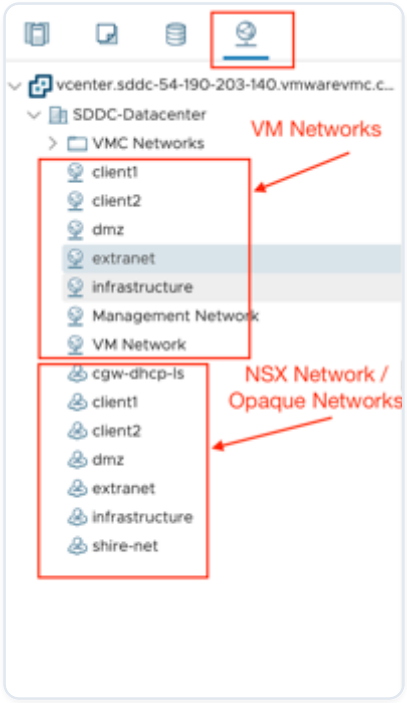
- Visualização de VM e Modelo: O administrador da nuvem pode criar muitas pastas.



- 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.

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 de 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.

Limitação

A partir do Citrix Virtual Apps and Desktops 2203 LTSR e posterior, o plug-in MCS AWS faz a chamada de API AWS `DescribeInstanceTypes` e, se for bem-sucedida, o MCS usa o nome de inventário criado a partir da resposta da API.

Portanto, ao fazer upgrade do CVAD 1912 para 2203 ou posterior, desabilite a permissão `DefineInstanceType` no AWS e, em seguida, atualize o catálogo existente usando o comando `Set-ProvScheme` para corresponder ao esquema de nomenclatura do 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 do AWS.

Visão geral da tarefa

Configure uma nuvem privada virtual (VPC) com sub-redes públicas e privadas. Ao concluir esta tarefa, o 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 desabilitado 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 unir instâncias ao domínio.

Tarefa 1: Configurar a VPC

1. No console de gerenciamento da AWS, selecione **VPC**.
2. No Painel da VPC, selecione **Criar VPC**.
3. Selecione **VPC e mais**.
4. Em NAT gateways ($), selecione **Em 1 AZ** ou **1 por AZ**.
5. Em opções de DNS, deixe **Habilitar nomes de host DNS** selecionado.
6. Selecione **Criar VPC**. A AWS cria as sub-redes públicas e privadas, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

Tarefa 2: Configurar grupos de segurança

Esta tarefa cria e configura os seguintes grupos de segurança para sua VPC:

- Um grupo de segurança público para associar às instâncias em sua sub-rede pública.
- Um grupo de segurança privado para associar às instâncias em sua sub-rede privada.

Para criar os grupos de segurança:

1. No Painel da VPC, selecione **Grupos de Segurança**.

2. Crie um grupo de segurança para o grupo de segurança público. Selecione **Criar Grupo de Segurança** e insira uma tag de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Sim, Criar**.

Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	ORIGEM
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	Selecione o grupo de segurança Público.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Confiabilidade da Sessão)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Quando terminar, selecione **Salvar**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	DESTINO
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	0.0.0.0/0
ICMP	0.0.0.0/0

5. Quando terminar, selecione **Salvar**.

Configurar o grupo de segurança privado

1. Na lista de grupos de segurança, selecione o grupo de segurança Privado.
2. Se você não configurou o tráfego do grupo de segurança público, você deve definir as portas TCP; selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	ORIGEM
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	Selecione o grupo de segurança Público.
ICMP	Selecione o grupo de segurança Público.
TCP 53 (DNS)	Selecione o grupo de segurança Público.
UDP 53 (DNS)	Selecione o grupo de segurança Público.
80 (HTTP)	Selecione o grupo de segurança Público.
TCP 135	Selecione o grupo de segurança Público.
TCP 389	Selecione o grupo de segurança Público.
UDP 389	Selecione o grupo de segurança Público.
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.

TIPO	DESTINO
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

Execute as seguintes etapas para criar duas instâncias EC2 e descriptografar a senha padrão do Administrador que a Amazon gera:

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No Painel do EC2, selecione **Iniciar Instância**.
3. Selecione uma imagem de máquina do Windows Server e o tipo de instância.
4. Na página **Configure Instance Details**, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Sub-rede**, faça as seguintes seleções para cada instância:
   - Host bastion: Selecione a sub-rede Pública
   - Controlador de Domínio: Selecione a sub-rede Privada
6. Em **Atribuir automaticamente endereço IP público**, faça as seguintes seleções para cada instância:
   - Host de bastião: Selecione **Habilitar.**
   - Controlador de Domínio: Selecione **Usar configuração padrão** ou **Desabilitar**.
7. Em **Interfaces de Rede**, insira um endereço IP primário dentro do intervalo de IP da sua sub-rede privada para 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 de Administrador padrão para a instância.
13. Selecione **Iniciar Instâncias**. selecione **Visualizar Instâncias** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-iniciada tenha passado em todas as verificações de status antes de acessá-la.
14. Adquira a senha de Administrador padrão para cada instância:
    a. Na lista de instâncias, selecione a instância e, em seguida, selecione **Conectar**.
    b. Vá para a guia **Cliente RDP**, selecione **Obter Senha** e carregue seu arquivo de chave privada (`.pem`) quando solicitado.
    c. Selecione **Descriptografar Senha** para obter a senha legível. A AWS exibe a senha padrão.
15. Repita as etapas a partir da etapa 2 até que você tenha criado duas instâncias:
    - Uma instância de host bastion em sua sub-rede pública
    - Uma instância em sua sub-rede privada que será usada como um 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 então 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. Da instância do host de bastião, 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 habilitadas 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.

Criar uma conexão

Ao criar uma conexão a partir do Studio:

- Você deve fornecer os valores da chave de API e da chave secreta. Você pode exportar o arquivo de chave contendo esses valores do AWS e depois importá-los. Você também deve

fornecer a região, zona de disponibilidade, nome da VPC, endereços de sub-rede, nome de domínio, nomes de grupos de segurança e credenciais.

- O arquivo de credenciais para a conta raiz do AWS (recuperado do console do AWS) não é formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão do AWS. Portanto, o 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).

Nota:

Depois de criar uma conexão, as tentativas de atualizar a chave de API e a chave secreta podem falhar. Para resolver o problema, verifique as restrições do seu servidor proxy ou firewall e certifique-se de que o seguinte endereço pode ser contatado: `https://*.amazonaws.com`.

Valores padrão de conexão de host

Ao criar conexões de host em ambientes de nuvem AWS, os seguintes valores padrão são exibidos:

OPÇÃO	ABSOLUTO	PORCENTAGEM
Ações simultâneas (todos os tipos)	125	100
Máximo de novas ações por minuto	125	

O MCS suporta 100 operações de provisionamento simultâneas máximas por padrão.

URL do endpoint de serviço

URL de endpoint de serviço de 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.

Locação AWS

O AWS oferece as seguintes opções de locação: locação compartilhada (o tipo padrão) e locação dedicada. Locação compartilhada significa que várias instâncias do Amazon EC2 de diferentes clientes podem residir na mesma peça de hardware físico. Locação dedicada significa que suas instâncias EC2 são executadas apenas em hardware com outras instâncias que você implantou. Outros clientes não usam a mesma peça de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando o PowerShell.

Configurar a locação de host dedicado do AWS usando o PowerShell

Você pode criar um catálogo de máquinas com locação de host definida através do PowerShell.

Um host dedicado Amazon é um servidor físico com capacidade de instância que é totalmente dedicado, permitindo que você use licenças de software existentes por soquete ou por VM.

Hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado de tipos de instância C4 Large é limitado a executar 16 instâncias. Consulte o site da AWS para obter mais informações.

Os requisitos para provisionamento em hosts da AWS incluem:

- Uma imagem BYOL (traga sua própria licença) importada (AMI). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para satisfazer as solicitações de provisionamento.
- habilitar **auto-placement**.

Para provisionar para um host dedicado na AWS usando PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro TenancyType definido como *Host*.

Consulte a Citrix Developer Documentation para obter mais informações.

Captura de propriedades de instância AWS

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, você seleciona uma AMI para representar a imagem mestre/dourada desse catálogo. Dessa AMI, o MCS usa um instantâneo do disco. Em versões anteriores, se você quisesse funções ou

tags em suas máquinas, você usaria o console da AWS para configurá-las individualmente. Essa funcionalidade é habilitada por padrão.

> **Dica:**

> Para usar a captura de propriedades de instância 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 da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturadas.

As propriedades capturadas incluem:

- Funções IAM – aplicadas a instâncias provisionadas.
- Tags - aplicadas a instâncias provisionadas, seus discos e NICs. Essas tags são aplicadas a recursos transitórios do Citrix®, incluindo: bucket e objetos S3, recursos de volume e worker, e AMIs, instantâneos e modelos de inicialização.

> **Dica:**

> A marcação de recursos transitórios do Citrix é opcional e configurável usando a propriedade personalizada `AwsOperationalResourcesTagging`.

Capturando a propriedade da instância 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 Citrix Developer Documentation para obter mais informações.

Aplicando propriedades de instância AWS e marcando recursos operacionais

Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode controlar se as propriedades de função IAM e tag serão aplicadas a essas máquinas. Você também pode controlar se as tags da máquina serão aplicadas aos recursos operacionais.

Marcação de recursos operacionais AWS

Uma Amazon Machine Image (AMI) representa um tipo de appliance virtual usado para criar uma máquina virtual dentro do ambiente Amazon Cloud, comumente referido como EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Ao criar um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem dourada para esse catálogo.

> **Importante:**
>
> A criação de catálogos capturando uma propriedade de instância e um modelo de inicialização é necessária para usar a marcação de recursos operacionais.

> Para criar um catálogo AWS, você deve primeiro criar uma AMI para a instância que deseja que seja a imagem dourada. O MCS lê as tags dessa instância e as incorpora ao modelo de inicialização. As tags do modelo de inicialização são então aplicadas a todos os recursos Citrix criados em seu ambiente AWS, incluindo:

- Máquinas Virtuais
- Discos de VM
- Interfaces de rede de VM
- Buckets S3
- Objetos S3
- Modelos de inicialização
- AMIs

Marcando 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>
```

Definindo permissões IAM

Use as informações nesta seção para definir permissões IAM para o Citrix DaaS no 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.

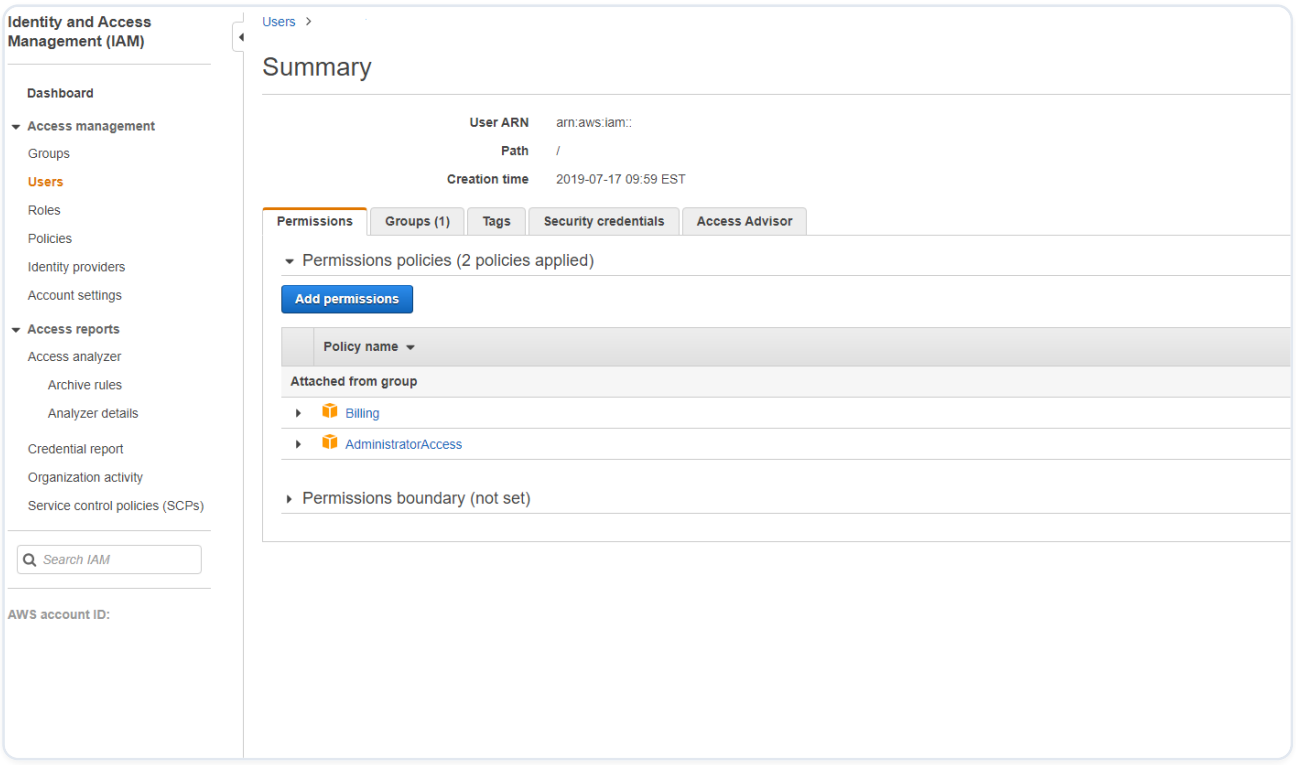
Após inserir as informações da política, selecione **Continuar** para concluir o grupo de usuários. Os usuários do grupo recebem permissões para executar apenas as ações necessárias para o Citrix DaaS.

> **Importante:**
>
> Use o texto da política fornecido no exemplo acima para listar as ações que um Citrix DaaS usa para executar ações em uma conta AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar mais restrições aos recursos.

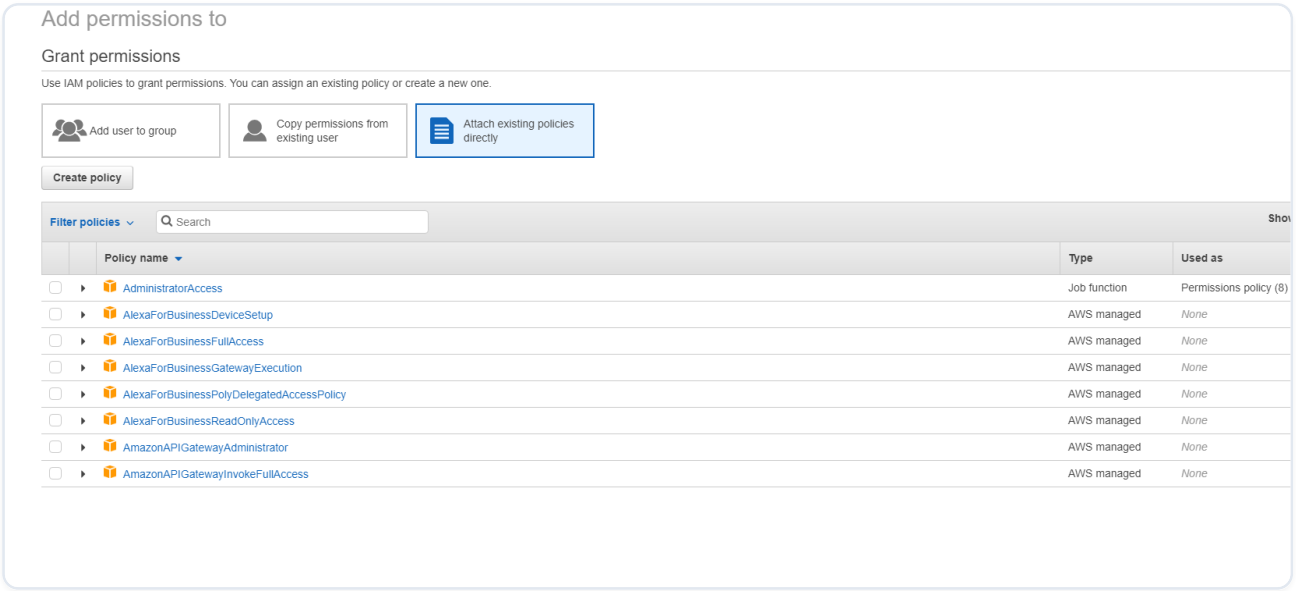
Adicionando permissões IAM

Defina as permissões na seção **IAM** do Console de Gerenciamento da AWS:

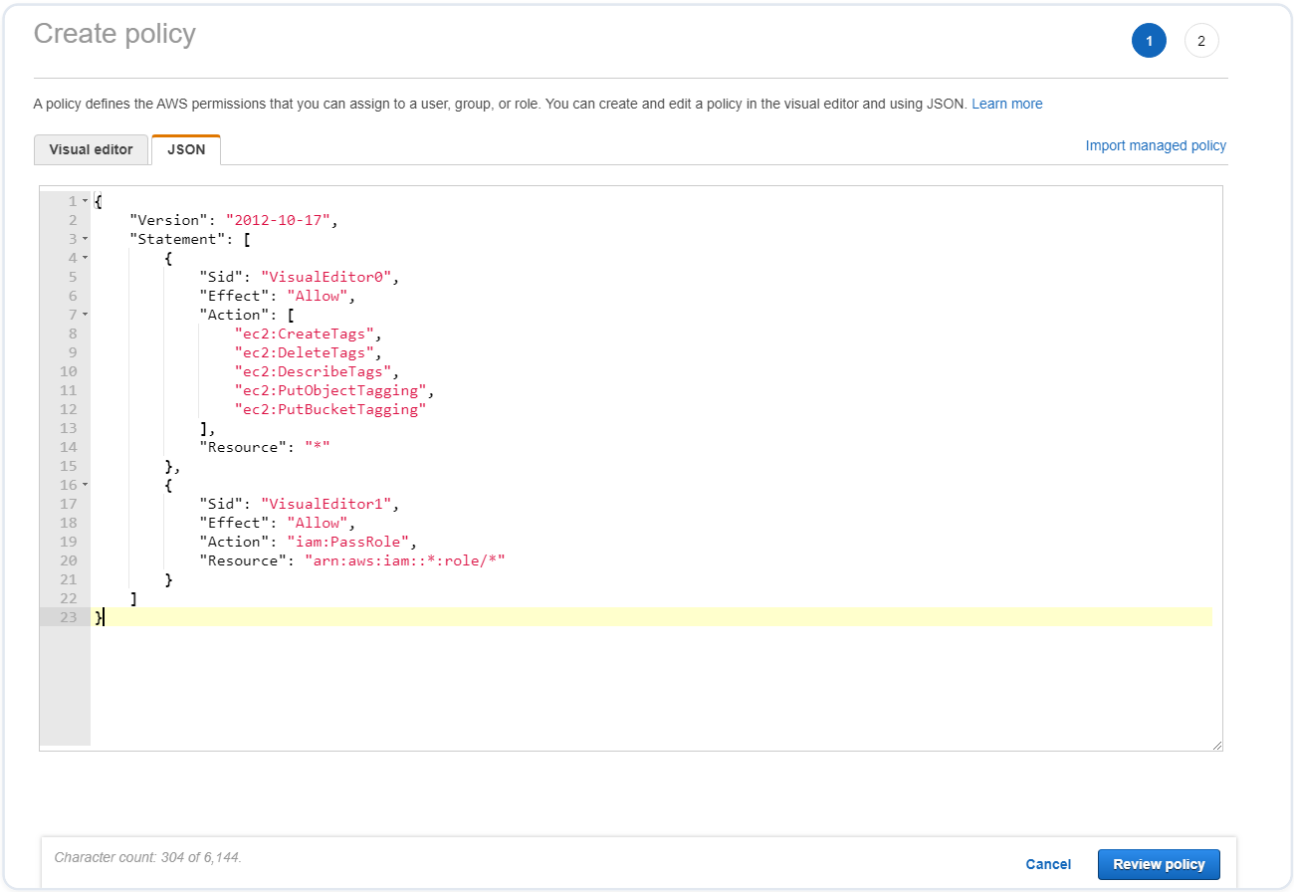
1. No painel **Resumo**, selecione a guia **Permissões**.
2. Selecione **Adicionar permissões.**



Na tela **Adicionar Permissões a**, conceda permissões:



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



Dica:

O exemplo JSON mencionado pode não incluir todas as permissões para o seu ambiente. Consulte Como Definir Permissões de Gerenciamento de Acesso de Identidade Executando Citrix Virtual Apps and Desktops no AWS para obter mais informações.

Sobre permissões AWS

Esta seção contém a lista completa de permissões da 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 obtidas da 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"
            ],
            "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:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "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 SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.

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.

As seguintes permissões devem ser adicionadas à política:

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

> **Importante:**
>
> - Você pode adicionar uma nova VM a catálogos de máquinas existentes sem qualquer operação de volume worker, como volume worker AMI e volume worker VM.
> - Se você excluir um catálogo existente que usava volume worker anteriormente, todos os artefatos, incluindo os relacionados ao volume worker, serão excluídos.

Criptografia EBS de volumes criados

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

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

Observação:

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

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }
```

```
        }

    ]

}
```

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

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

Para obter mais informações, consulte a documentação oficial do AWS Key Management Service.

Autenticação baseada em função do IAM

As seguintes permissões são adicionadas para suportar a autenticação baseada em função.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {
```

```
            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

Política de permissões mínimas do IAM

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

Importante:

Para usar **role_based_auth**, primeiro configure a função IAM desejada na instância EC2 do conector de nuvem ao configurar o conector de nuvem. Usando o Citrix Studio, adicione a conexão de hospedagem e forneça o role_based_auth para a chave de autenticação e o segredo. Uma conexão de hospedagem com essas configurações usa então a autenticação baseada em função.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",
```

```
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "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:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

Observação:

- A seção EC2 relacionada a SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.
- A seção KMS é necessária apenas ao usar a criptografia de volume EBS.
- A seção de permissão iam:PassRole é necessária apenas para **role_based_auth**.
- Permissões específicas em nível de recurso podem ser adicionadas em vez de acesso total, com base em seus requisitos e ambiente. Consulte os documentos da AWS Demystifying EC2 Resource-Level Permissions e Access management for AWS resources para obter mais detalhes.

Mais informações

- 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. Este artigo o orienta no uso do Machine Creation Services (MCS) para provisionar máquinas virtuais em sua implantação de serviço Citrix Virtual Apps ou Citrix Virtual Desktops.

Requisitos

- Conta do Citrix Cloud™. O recurso descrito neste artigo está disponível apenas no Citrix Cloud.
- Assinatura do Citrix DaaS. Para obter detalhes, consulte Introdução.
- Um projeto do Google Cloud. O projeto armazena todos os recursos de computação associados ao catálogo de máquinas. Pode ser um projeto existente ou um 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 a conta de serviço do Google Cloud.
- Habilite o acesso privado do Google. Para obter detalhes, consulte Habilitar acesso privado do Google.

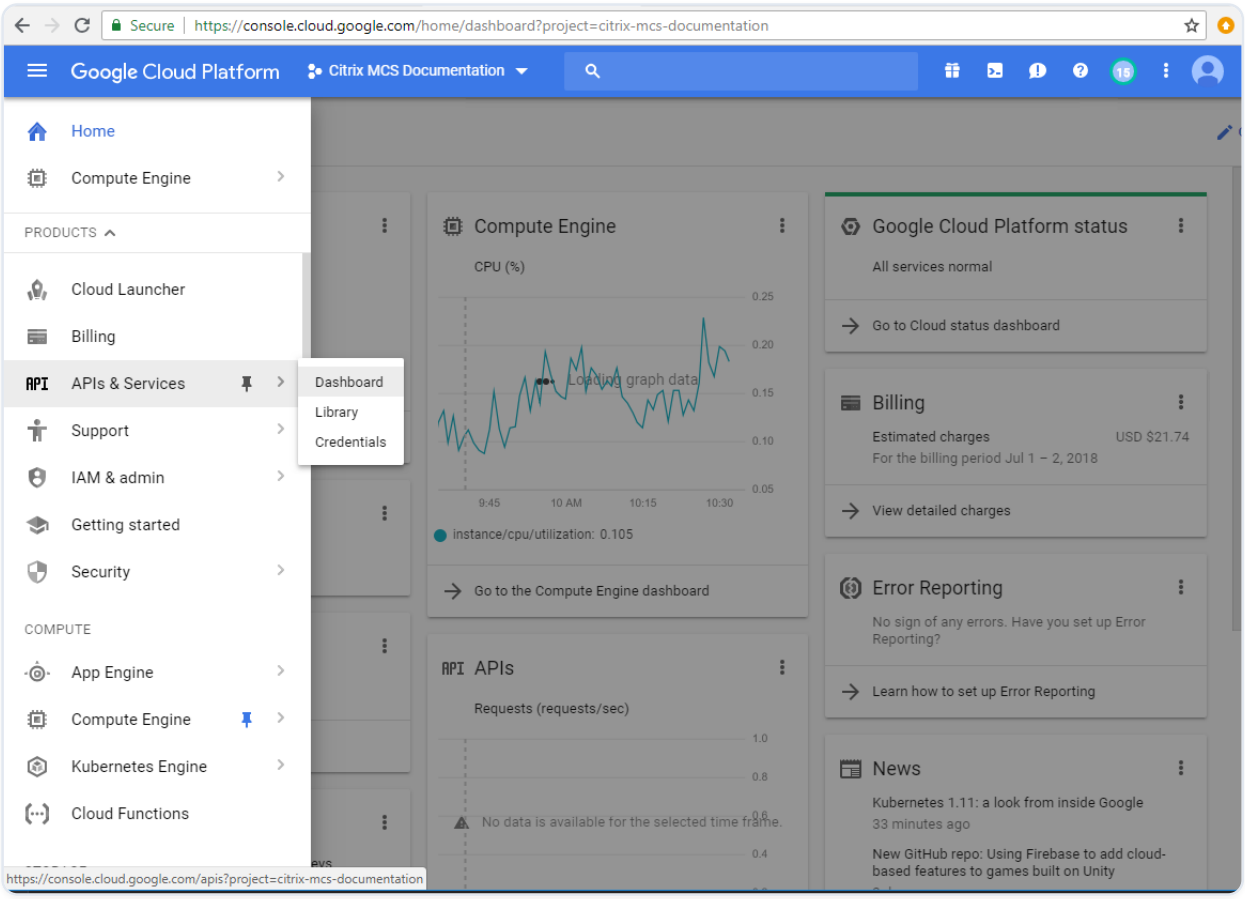
Habilitar APIs do Google Cloud

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

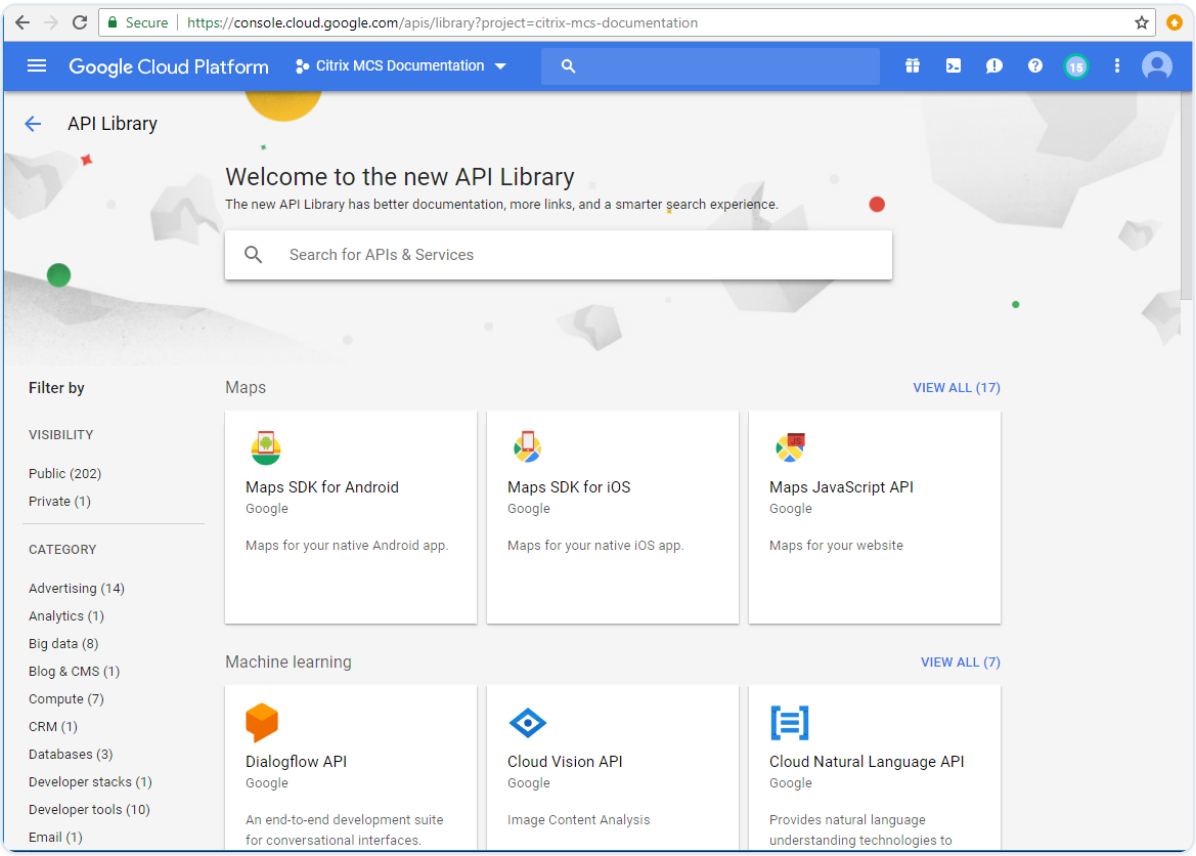
No console do Google Cloud, conclua estas etapas:

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 **API do Compute Engine**.

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 **API do Cloud Resource Manager**.

d. Na página **Cloud Resource Manager API**, selecione **Enable**. O status da API é exibido.

4. Da mesma forma, habilite a **API Identity and Access Management (IAM)** e a **API Cloud Build**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para fazer isso:

1. Abra o Google Console e carregue o Cloud Shell.
2. Execute os quatro comandos a seguir no Cloud Shell:

- gcloud services enable compute.googleapis.com.
- gcloud serviços habilitar cloudresourcemanager.googleapis.com

- gcloud serviços habilitar iam.googleapis.com
- gcloud serviços habilitar cloudbuild.googleapis.com

3. Clique em **Autorizar** se o Cloud Shell solicitar.

Configurar e atualizar contas de serviço

> **Observação:**
>
> O GCP está introduzindo alterações no comportamento padrão do Cloud Build Service e no uso de contas de serviço após April 29, 2024. Para obter mais informações, consulte Cloud Build Service Account Change. Seus projetos existentes do Google com a API do Cloud Build ativada antes de April 29, 2024 não são afetados por essa alteração. No entanto, se você quiser manter o comportamento existente do Cloud Build Service após April 29, poderá criar ou aplicar a política da organização para desativar a imposição de restrições antes de ativar a API do Cloud Build. Como resultado, o conteúdo a seguir é dividido em dois: Before April 29, 2024 e After April 29, 2024. Se você definir a nova política da organização, siga a seção Before 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**.

   > **Observação:**
   >
   > Habilite todas as APIs para obter a lista completa de funções.

Após April 29, 2024

O Citrix Cloud usa duas contas de serviço separadas dentro do projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Admin > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar a função de **Administrador de Armazenamento** que requer as seguintes permissões:
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get

- storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com.`.

Verifique se a conta de serviço recebeu as seguintes funções.

- Conta de Serviço do Cloud Build
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

   Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

   - Administrador de Computação
   - Administrador de Armazenamento
   - Editor do Cloud Build
   - Usuário da Conta de Serviço
   - Usuário do Cloud Datastore
   - Cloud KMS Crypto Operator

   O Cloud KMS Crypto Operator requer as seguintes permissões:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get

- cloudkms.keyRings.list

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.
- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da conta de serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado 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 COMPUTE

Para adicionar funções à Conta de Serviço do Cloud Compute:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a Conta de Serviço do Cloud Compute, identificável por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**.

   Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

Observação:

Habilite todas as APIs para obter a lista completa de funções.

Permissões de armazenamento e gerenciamento de bucket

O Citrix DaaS melhora o processo de relatório de falhas de compilação na nuvem para o serviço Google Cloud. Este serviço executa compilações no Google Cloud. O Citrix DaaS cria um bucket de armazenamento chamado `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` onde os serviços do Google Cloud capturam informações de log de compilação. Uma opção é definida neste bucket que exclui o conteúdo após um período de 30 dias. Este processo exige que a conta de serviço usada para a conexão tenha as permissões do Google Cloud definidas como `storage.buckets.update`. Se a conta de serviço não tiver essa permissão, o Citrix DaaS ignora os erros e prossegue com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de compilação aumenta e requer limpeza manual.

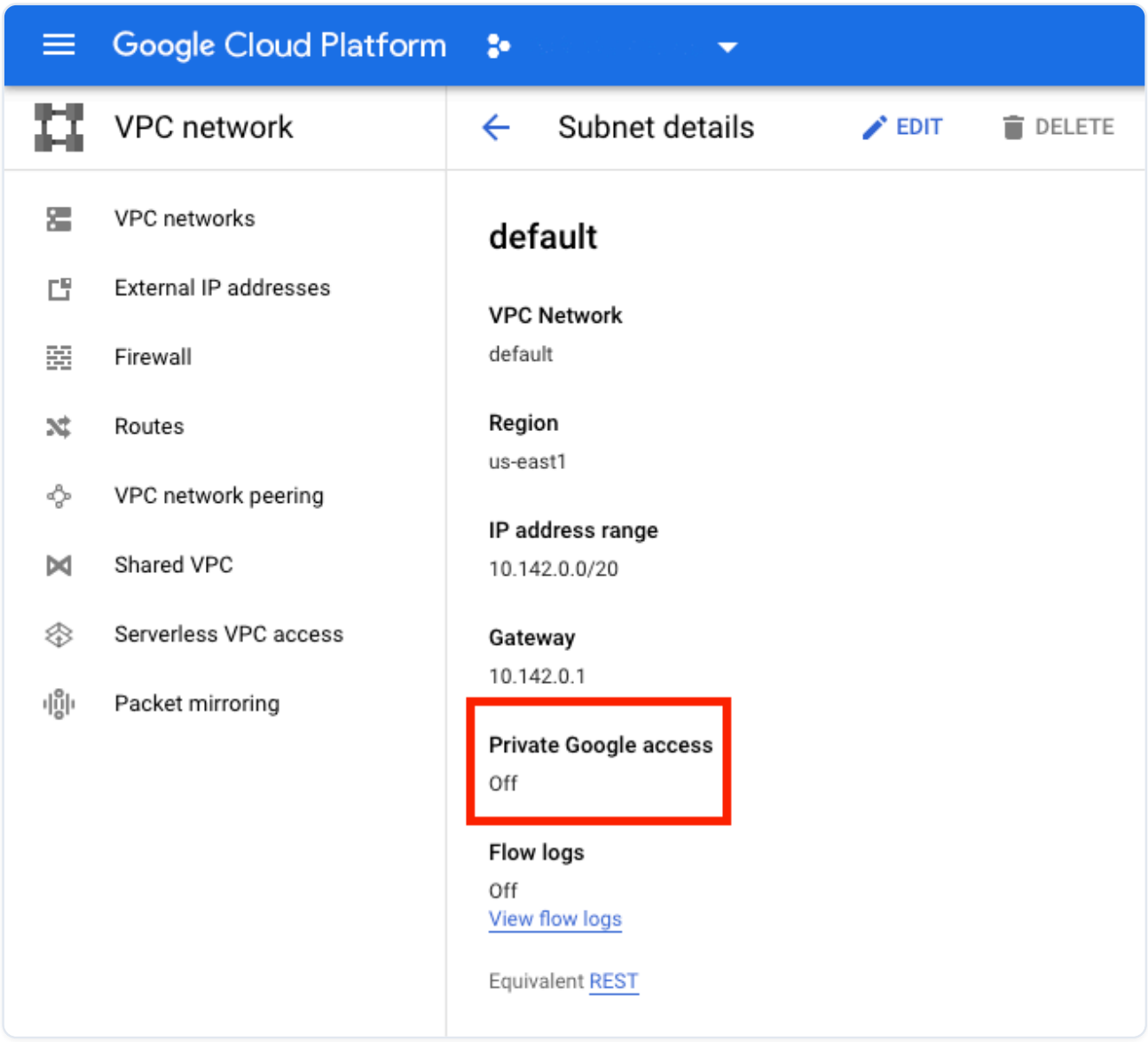
Habilitar acesso privado do Google

Quando uma VM não possui um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Ao habilitar o acesso privado, a VM se conecta ao conjunto de endereços IP externos usados pela API do Google e serviços associados.

> **Nota:**
>
> Independentemente de o acesso privado do Google estar ativado, todas as VMs com e sem endereços IP públicos devem ser capazes de acessar as APIs Públicas do Google, especialmente se dispositivos de rede de terceiros tiverem sido instalados no ambiente.

Para garantir que uma VM 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.

Adicionar uma conexão

Siga as orientações em Criar uma conexão e recursos. A descrição a seguir o orienta na configuração de uma conexão de hospedagem:

1. Em **Gerenciar > Configuração**, selecione **Hospedagem** no painel esquerdo.
2. Selecione **Adicionar Conexão e Recursos** na barra de ações.

3. Na página **Conexão**, selecione **Criar uma nova Conexão** e **ferramentas de provisionamento Citrix™**, e então selecione **Avançar**.
    - **Tipo de conexão**. Selecione **Google Cloud** no menu.
    - **Nome da conexão**. Digite um nome para a conexão.
4. Na página **Região**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Avançar**.
5. Na página **Rede**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Avançar**. O nome do recurso ajuda a identificar a combinação de região e rede. Redes virtuais com o sufixo *(Compartilhado)* anexado ao seu nome representam VPCs compartilhadas. Se você configurar uma função IAM no nível da sub-rede para uma VPC compartilhada, apenas sub-redes específicas da VPC compartilhada aparecerão na lista de sub-redes.

    > **Nota:**
    >
    > - O nome do recurso pode conter 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

6. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir** para sair da janela **Adicionar Conexão e Recursos**.

Após criar a conexão e os recursos, a conexão e os recursos 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.

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 snapshot do disco. Isso permite que você use uma convenção de nomenclatura significativa para rastrear versões, oferece mais opções para gerenciar versões anteriores de sua imagem mestre e economiza tempo na criação do catálogo de máquinas. Se você não criar seu próprio snapshot, o MCS criará um snapshot temporário para você (que é excluído ao final do processo de provisionamento).

Criar um catálogo de máquinas

> **Nota:**

> Crie seus recursos antes de criar um catálogo de máquinas. Use as convenções de nomenclatura estabelecidas pelo Google Cloud ao configurar catálogos de máquinas. Consulte Diretrizes de nomenclatura de buckets e objetos para obter mais informações.

> Siga as orientações em Criar catálogos de máquinas. Atualmente, o Studio não oferece suporte à criação de catálogos do Google Cloud. Use o PowerShell em vez disso.

Gerenciar catálogo de máquinas

Para adicionar máquinas a um catálogo, atualizar máquinas e reverter uma atualização, consulte Gerenciar catálogos de máquinas.

Gerenciamento de energia

O Citrix DaaS permite o gerenciamento de energia de suas máquinas do Google Cloud. Use o nó **Pesquisar** no painel de navegação 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 o consumo de energia de 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 Autoscale.

Proteger a exclusão acidental de máquinas

O Citrix DaaS permite proteger recursos do MCS no Google Cloud para evitar exclusão acidental. Configure a VM provisionada definindo o sinalizador `deletionProtection` como TRUE.

Por padrão, as VMs provisionadas por meio do plug-in MCS ou Google Cloud são criadas com o InstanceProtection habilitado. 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` habilitado.

Se você tentar excluir uma instância de VM para a qual você definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você tiver a permissão `compute.instances.setDeletionProtection` ou a função IAM de **Administrador de Computação** atribuída, poderá redefinir o sinalizador para permitir que o recurso seja excluído.

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*. Em seguida, você pode reiniciar manualmente as máquinas do Google Cloud por meio do Citrix DaaS. Com esse recurso, você pode:

- Importar máquinas de SO multi-sessão do Google Cloud criadas manualmente para um catálogo de máquinas do Citrix Virtual Apps and Desktops.
- Remover máquinas de SO multi-sessão do Google Cloud criadas manualmente de um catálogo do Citrix Virtual Apps and Desktops.
- Usar os recursos de gerenciamento de energia existentes do Citrix Virtual Apps and Desktops para gerenciar a energia de máquinas de SO multi-sessão do Google Cloud Windows. Por exemplo, defina um agendamento de reinicialização 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 esse recurso, o Machine Creation Services™ (MCS) oferece suporte ao provisionamento e gerenciamento de catálogos de máquinas implantados em VPCs Compartilhadas. Esse 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. Esse processo permite que o MCS acesse e use os 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 de host. Essas permissões adicionais devem ser concedidas a quaisquer contas de serviço usadas para criar conexões de host baseadas em VPC Compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas para o Citrix DaaS. Elas são usadas para facilitar a implementação de VPCs locais. Com as VPCs Compartilhadas, essas permissões adicionais permitem o acesso a outros recursos de VPC compartilhados.

> Um máximo de quatro permissões extras devem ser concedidas à conta de serviço associada à conexão do host para suportar o VPC Compartilhado:

1. **compute.firewalls.list** - Esta permissão é obrigatória. Ela permite que o MCS recupere a lista de regras de firewall presentes no VPC Compartilhado.
2. **compute.networks.list** - Esta permissão é obrigatória. Ela permite que o MCS identifique as redes VPC Compartilhadas disponíveis para a conta de serviço.
3. **compute.subnetworks.list** – Esta permissão é opcional, dependendo de como você usa os VPCs. Ela permite que o MCS identifique as sub-redes dentro dos VPCs Compartilhados visíveis. Esta permissão já é exigida ao usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.
4. **compute.subnetworks.use** - Esta permissão é opcional, dependendo de como você usa os VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionados. Esta permissão já é exigida para usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.

Ao usar essas permissões, considere que existem diferentes abordagens com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão em nível de projeto:
  - Permite acesso a todos os VPCs Compartilhados dentro do projeto host.
  - Requer que as permissões #3 e #4 sejam atribuídas à conta de serviço.
- Permissão em nível de sub-rede:
  - Permite acesso a sub-redes específicas dentro do VPC Compartilhado.

- As permissões #3 e #4 são intrínsecas à atribuição em nível de sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que melhor se adapta às suas necessidades organizacionais e padrões de segurança.

> **Dica:**
>
> Para obter mais informações sobre as diferenças entre permissões em nível de projeto e em nível de sub-rede, consulte a documentação do Google Cloud.

Regras de Firewall

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como disco 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; uma para tráfego de entrada e outra para tráfego de saída. Ao usar VCPs locais do Google Cloud, o MCS cria esse firewall na rede local e o aplica à máquina para a masterização. Após a conclusão da masterização, a regra de firewall é removida da imagem.

Recomendamos manter o número de novas permissões necessárias para usar VPCs Compartilhadas no mínimo. As VPCs Compartilhadas são recursos corporativos de nível superior e geralmente possuem protocolos de segurança mais rígidos em vigor. Por esse motivo, crie um par de regras de firewall no projeto host nos recursos da VPC compartilhada, uma para entrada e outra para saída. Atribua a mais alta prioridade a elas. Aplique uma nova tag de destino a cada uma dessas regras, usando o seguinte valor:

`citrix-provisioning-quarantine-firewall`

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura por regras de firewall que contenham esta tag de destino. Em seguida, ele examina as regras quanto à correção e as aplica à máquina usada para preparar a imagem mestre para o catálogo. Se as regras de firewall não forem encontradas, ou se as regras forem encontradas, mas as regras ou suas prioridades estiverem incorretas, uma mensagem semelhante à seguinte aparecerá:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC
<name> in project <project>. " Please ensure you have created 'deny all' firewall
```

`rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

Configurando a VPC compartilhada

Antes de adicionar a VPC Compartilhada como uma conexão de host no Web Studio, conclua as seguintes etapas para adicionar contas de serviço do projeto no qual você pretende provisionar:

1. Crie uma função IAM.
2. Adicione a conta de serviço usada para criar uma conexão de host CVAD à função IAM do projeto host da VPC Compartilhada.
3. Adicione a conta de serviço do Cloud Build do projeto no qual você pretende provisionar à função IAM do projeto host da VPC Compartilhada.
4. Crie regras de firewall.

CRIAR UMA FUNÇÃO IAM

Determine o nível de acesso da função — *acesso em nível de projeto* ou um modelo mais restrito usando *acesso em nível de sub-rede*.

Acesso em nível de projeto para função IAM. Para a função IAM em nível de projeto, inclua as seguintes permissões:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função IAM em nível de projeto:

1. No console do Google Cloud, navegar até **IAM e administrador > Funções**.
2. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
3. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

Função IAM em nível de sub-rede. Esta função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` após selecionar **CRIAR FUNÇÃO**. Para este nível de acesso IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função IAM em nível de sub-rede:

1. No console do Google Cloud, navegar até **Rede VPC** > **VPC compartilhada**. A página **VPC compartilhada** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.
2. Na página **VPC Compartilhada**, selecione a sub-rede que você deseja acessar.
3. No canto superior direito, selecione **ADICIONAR MEMBRO** para adicionar uma conta de serviço.
4. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar um papel** e, em seguida, **Usuário da Rede de Computação**.
    c. Selecione **SALVAR**.
5. No console do Google Cloud, navegar para **IAM e Administrador** > **Funções**.
6. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
7. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

ADICIONAR UMA CONTA DE SERVIÇO À FUNÇÃO IAM DO PROJETO HOST

Após criar uma função IAM, siga as etapas abaixo para adicionar uma conta de serviço para o projeto host:

1. No console do Google Cloud, navegar para o projeto host e, em seguida, para **IAM e Administrador > IAM**.
2. Na página **IAM**, selecione **ADICIONAR** para adicionar uma conta de serviço.

3. Na página **Adicionar membros**:

    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.

    b. Selecione um campo de função, digite a função IAM que você criou e selecione a função no menu.

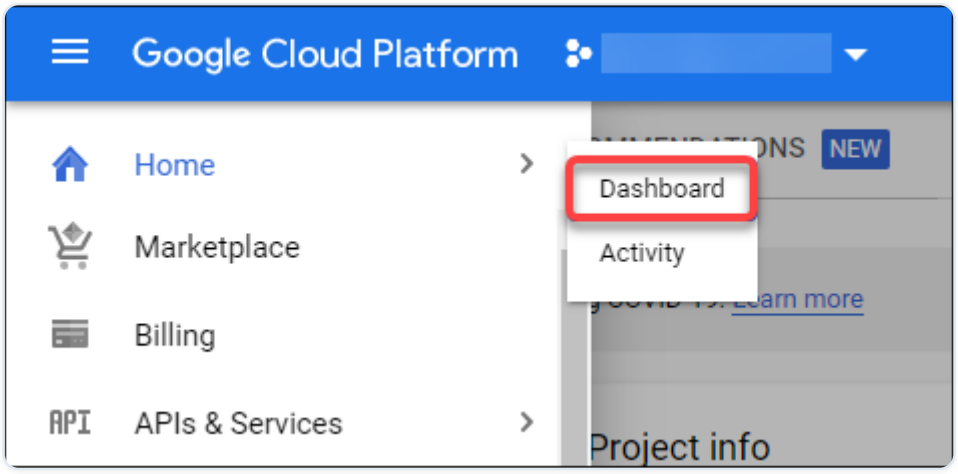
    c. Selecione **SALVAR**.

A conta de serviço agora está configurada para o projeto host.

ADICIONAR A CONTA DE SERVIÇO DE COMPILAÇÃO EM NUVEM AO VPC COMPARTILHADO

Cada assinatura do Google Cloud tem uma conta de serviço que é nomeada após o número de ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar qual é o número de ID do projeto para o seu projeto selecionando **Início** e **Painel** 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 de máquina selecionada e a usa para preparar o disco do sistema da imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que então executa scripts de preparação. Essa VM deve ser executada em um ambiente isolado que proíba todo o tráfego de rede de entrada e saída. Para criar um ambiente isolado, o MCS requer duas regras de firewall de *negação total* (uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall no *Projeto Host* da seguinte forma:

1. No console do Google Cloud, navegar até o projeto host e depois para **Rede VPC > Firewall**.
2. Na página **Firewall**, selecione **CRIAR REGRA DE FIREWALL**.
3. Na página **Criar uma regra de firewall**, preencha o seguinte:
   - **Nome**. Digite um nome para a regra.
   - **Rede**. Selecione a rede VPC Compartilhada à qual a regra de firewall de entrada se aplica.
   - **Prioridade**. Quanto menor o valor, maior a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
   - **Direção do tráfego**. Selecione **Entrada**.
   - **Ação na correspondência**. Selecione **Negar**.
   - **Destinos**. Use o padrão, **Tags de destino especificadas**.
   - **Tags de destino**. Digite `citrix-provisioning-quarantine-firewall`.
   - **Filtro de origem**. Use o padrão, **Intervalos de IP**.
   - **Intervalos de IP de origem**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
   - **Protocolos e portas**. Selecione **Negar tudo**.
4. Selecione **CRIAR** para criar a regra.
5. Repita os passos 1 a 4 para criar outra regra. Para **Direção do tráfego**, selecione **Saída**.

ADICIONAR UMA CONEXÃO

Adicione uma conexão aos ambientes do Google Cloud. Consulte Adicionar uma conexão.

Habilitar seleção de zona

O Citrix Virtual Apps and Desktops oferece suporte à seleção de zona. Com a seleção de zona, você especifica as zonas onde deseja criar VMs. Com a seleção de zona, os administradores podem colocar nós de locatário único em zonas de sua escolha. Para configurar a locação única, você deve concluir o seguinte no Google Cloud:

- Reservar um nó de locatário único do Google Cloud
- Criar a imagem mestre do VDA

Reservando um nó de locatário único do Google Cloud

Para reservar um nó de locatário único, consulte a documentação do Google Cloud.

> **Importante:**

> Um modelo de nó é usado para indicar as características de desempenho do sistema que é reservado no grupo de nós. Essas características incluem o número de vGPUs, a quantidade de memória alocada ao nó e o tipo de máquina usado para máquinas criadas no nó. Para obter mais informações, consulte a documentação do Google Cloud.

Criando a imagem mestre do VDA

Para implantar máquinas no nó de locatário único com sucesso, você precisa seguir etapas extras ao criar uma imagem mestre de VM. As instâncias de máquina no Google Cloud têm uma propriedade chamada *rótulos de afinidade de nó*. As instâncias usadas como imagens mestras para catálogos implantados no nó de locatário único exigem um *rótulo de afinidade de nó* que corresponda ao nome do **grupo de nós de destino**. Para conseguir isso, tenha em mente o seguinte:

- Para uma nova instância, defina o rótulo no console do Google Cloud ao criar uma instância. Para obter detalhes, consulte Definir um rótulo de afinidade de nó ao criar uma instância.
- Para uma instância existente, defina o rótulo usando a linha de comando **gcloud**. Para obter detalhes, consulte Definir um rótulo de afinidade de nó para uma instância existente.

> **Nota:**

> Se você pretende usar a locação única com uma VPC compartilhada, consulte Virtual Private Cloud Compartilhada.

DEFINIR UM RÓTULO DE AFINIDADE DE NÓ AO CRIAR UMA INSTÂNCIA

Para definir o rótulo de afinidade de nó:

1. No console do Google Cloud, navegar até **Compute Engine > Instâncias de VM**.
2. Na página **Instâncias de VM**, selecione **Criar instância**.
3. Na página **Criação de instância**, digite ou configure as informações necessárias e, em seguida, selecione **gerenciamento, segurança, discos, rede, locação única** para abrir o painel de configurações.
4. Na guia **Locação única**, selecione **Procurar** para visualizar os grupos de nós disponíveis no projeto atual. A página **Nó de locatário único** é exibida, mostrando uma lista de grupos de nós disponíveis.
5. Na página **Nó de locatário único**, selecione o grupo de nós aplicável na lista e, em seguida, selecione **Selecionar** para retornar à guia **Locação única**. O campo de rótulos de afinidade de nó é preenchido com as informações selecionadas. Essa configuração garante que os catálogos de máquinas criados a partir da instância serão implantados no grupo de nós selecionado.
6. Selecione **Criar** para criar a instância.

DEFINIR UM RÓTULO DE AFINIDADE DE NÓ PARA UMA INSTÂNCIA EXISTENTE

Para definir o rótulo de afinidade de nó:

1. Na janela do terminal do Google Cloud Shell, use o comando *gcloud compute instances* para definir um rótulo de afinidade de nó. Inclua as seguintes informações no comando **gcloud**:

   - **Nome da VM**. Por exemplo, use uma VM existente chamada `s*2019-vda-base`.*
   - **Nome do grupo de nós**. Use o nome do grupo de nós que você criou anteriormente. Por exemplo, `mh-sole-tenant-node-group-1`.
   - **A zona onde a instância reside**. Por exemplo, a VM reside em `*us-east-1b* zone`.

   Por exemplo, digite o seguinte comando na janela do terminal:

   - `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

   Para obter mais informações sobre o comando *gcloud compute instances*, consulte a documentação do Google Developer Tools em `<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>`.

2. navegar para a página **Detalhes da instância da VM** da instância e verifique se o campo **Afinidades de Nó** é preenchido com o rótulo.

CRIAR UM CATÁLOGO DE MÁQUINAS

Depois de definir o rótulo de afinidade de nó, configure o catálogo de máquinas.

Visualização: Usando 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 DaaS deve ter as permissões corretas no projeto onde a chave está armazenada. Consulte Ajudando a proteger recursos usando chaves do Cloud KMS para obter mais informações.

Seu Agente de Serviço do Compute Engine está no seguinte formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato é diferente da Conta de Serviço padrão do Compute Engine.

> **Nota:**
>
> Esta Conta de Serviço do Compute Engine pode não aparecer na exibição **Permissões de IAM** do Google Console. Nesses casos, use o comando `gcloud` conforme descrito em Ajudando a proteger recursos usando chaves do Cloud KMS.

Atribuir permissões à conta do Citrix DaaS

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões KMS *no nível do projeto* ou permissões KMS *no nível do recurso*. Consulte Permissões e funções para obter mais informações.

PERMISSÕES NO NÍVEL DO PROJETO

Uma opção é fornecer à conta do Citrix DaaS permissões no nível do projeto para navegar pelos recursos do Cloud KMS. Para fazer isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua esta função personalizada à sua conta Citrix DaaS. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

PERMISSÕES NO NÍVEL DO RECURSO

Para a outra opção, permissões em nível de recurso, no console do Google Cloud, navegue até o `cryptoKey` que você usa para provisionamento MCS. Adicione a conta Citrix DaaS a um conjunto de chaves ou a uma chave que você usa para provisionamento de catálogo.

> **Dica:**
>
> Com esta opção, você não pode navegar por chaves regionais para seu projeto no inventário porque a conta do Citrix DaaS não tem permissões de lista no nível do 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 ANÉIS DE CHAVES

Anéis de chaves não podem ser renomeados ou excluídos. Além disso, você pode incorrer em cobranças imprevistas ao configurá-los. Ao excluir ou remover um anel 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 anel de chave do console.

Compatibilidade de acesso uniforme em nível de bucket

O Citrix DaaS é compatível com a política de controle de acesso uniforme no nível do bucket no Google Cloud. Essa funcionalidade aumenta o uso da política de IAM que concede permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com o controle de acesso uniforme no nível do bucket, o Citrix DaaS permite que você use uma lista de controle de acesso (ACL) para controlar o acesso a buckets de armazenamento ou objetos armazenados neles. Consulte Acesso uniforme no nível do bucket para obter informações gerais sobre o acesso uniforme no nível do bucket do Google Cloud. Para obter informações de configuração, consulte Exigir acesso uniforme no nível do bucket.

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.

Permissões GCP necessárias

Esta seção contém a lista completa de permissões GCP. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

> **Nota:**
>
> O GCP está introduzindo alterações no comportamento padrão e no uso de contas de serviço do Cloud Build Services após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build ativada antes de April 29, 2024 não são afetados por esta alteração. No entanto, se você quiser ter o comportamento existente do Cloud Build Service após April 29, poderá criar ou aplicar a política da organização para desativar a imposição da restrição antes de ativar a API. Se você definir a nova política da organização, ainda poderá seguir as permissões existentes nesta seção e os itens que estão marcados como **Antes da Alteração da Conta de Serviço do Cloud Build**. Caso contrário, siga as permissões existentes e os itens que estão marcados como **Após a Alteração da Conta de Serviço do Cloud Build**.

Criando uma conexão de host

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list
```

```
compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para Shared VPC para a Conta de Serviço do Citrix Cloud no projeto Shared VPC:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação

Gerenciamento de energia de VMs

Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento no caso de catálogos somente com gerenciamento de energia:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend
```

```
compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

Criar, atualizar ou excluir VMs

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete
```

```
compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create
```

```
compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list
```

```
compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Citrix Cloud no projeto de VPC Compartilhada para criar uma unidade de hospedagem usando VPC e sub-rede do projeto de VPC Compartilhada:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Usuário da Rede de Computação
  - Usuário do Cloud Datastore

- (Antes da alteração da conta de serviço do Cloud Build): Permissões mínimas necessárias para a Conta de Serviço do Cloud Build no projeto de Provisionamento, exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:
- (Após a alteração da conta de serviço do Cloud Build): Permissões mínimas necessárias para a Conta de Serviço do Cloud Compute no projeto de Provisionamento, exigidas pelo serviço Google Cloud Compute ao baixar o disco de instruções de preparação para o MCS:

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels
```

```
compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list
```

Os seguintes papéis definidos 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
```

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

- (Antes da alteração da conta de serviço do Cloud Build): Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Cloud Build no projeto de Provisionamento, exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:
- (Após a alteração da conta de serviço do Cloud Build): Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Cloud Compute no projeto de Provisionamento, exigidas pelo serviço Google Cloud Compute ao baixar o disco de instruções de preparação para o MCS:

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

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
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Visualizador de KMS de Computação

Permissões gerais

A seguir estão as permissões para a conta de serviço do Citrix Cloud no projeto de provisionamento para todos os recursos suportados no MCS. Essas permissões fornecem a melhor compatibilidade daqui para frente:

```
resourcemanager.projects.get

cloudbuild.builds.create
```

```
cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly
```

```
compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig
```

```
compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp
```

```
compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use
```

```
compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização Nutanix

Siga estas orientações ao usar o Nutanix Acropolis para fornecer máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™. O processo de configuração inclui as seguintes tarefas:

- Instale e registre o plug-in do Nutanix em seu ambiente Citrix Virtual Apps and Desktops.
- Crie uma conexão com o hipervisor Nutanix Acropolis.
- Crie um catálogo de máquinas que usa um instantâneo de uma imagem mestre que você criou no hipervisor Nutanix.

Para obter mais informações, consulte o Guia de Instalação do plug-in Nutanix Acropolis MCS, 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 do Nutanix em todos os seus Delivery Controllers. Use o Citrix Studio para criar uma conexão com o Nutanix. Em seguida, crie um catálogo de máquinas que usa um instantâneo de uma imagem mestre que você criou no ambiente Nutanix.

Dica:

Recomendamos que você pare e reinicie o Citrix Host Service, o Citrix Broker Service e o Machine Creation Services™ ao instalar ou atualizar o plug-in do Nutanix.

> Para obter informações sobre como instalar o plug-in do Nutanix, consulte o site de Documentação da Nutanix.

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, atentando-se aos 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 Xi** 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).

  > **Nota:**
  >
  > 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 DRaaS privados e públicos do Nutanix (`.pem`).

> **Dica:**
>
> Se você implantar máquinas usando Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

Criar um catálogo de máquinas usando um snapshot do Nutanix

As informações a seguir são um suplemento às orientações em Criar catálogos de máquinas. Para criar um catálogo, siga as orientações gerais desse artigo, observando os detalhes específicos 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 Mestra**, selecione o instantâneo da imagem. Os nomes de instantâneos do Acropolis devem ser prefixados com “XD_” para serem usados no Citrix Virtual Apps and Desktops. Use o console do Acropolis para renomear seus instantâneos, se necessário. Se você renomear instantâneos, reinicie o assistente de criação de 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 mestra 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.

Soluções de nuvem e parceiros Nutanix

O Citrix Virtual Apps and Desktops™ oferece suporte à seguinte solução de nuvem e parceira da Nutanix:

- Clusters de Nuvem Nutanix no AWS

Clusters de Nuvem Nutanix no AWS

O Citrix Virtual Apps and Desktops oferece suporte aos Nutanix Cloud Clusters 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 Nutanix Cloud Clusters no AWS, consulte Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Dica:**
>
> Este suporte oferece a mesma funcionalidade de um cluster Nutanix local. Apenas um único cluster é suportado, o *Prism Element*. Para obter mais informações, consulte aqui.

Requisitos

Você precisa do seguinte para usar os Clusters Nutanix no AWS:

- Uma conta Nutanix.
- Uma conta AWS com as seguintes permissões:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Criar um Cluster Nutanix

Para criar um Cluster Nutanix:

1. Faça login na sua conta Nutanix.
2. Localize a opção **Nutanix cluster** e clique em **Launch**. O **Nutanix Console** é aberto. Para obter mais informações, consulte Get Started with Nutanix Cluster on 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.
- Cluster Nutanix do Host - Nó `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- Cluster Nutanix do Host - 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.

Conectar ao Nutanix Prism

Depois de criar um cluster Nutanix, conecte-se ao Nutanix Prism.

Para conectar-se ao Nutanix Prism:

1. Crie uma VM bastion na sub-rede 10.0.129.0/24.
2. Faça RDP na VM bastion, vá para a URL do **Prism Element** que você copiou na seção anterior.
3. Faça login usando as credenciais padrão: `admin:nutanix/4u`. Lembre-se de alterar a senha.

Crie uma VM no Cluster Nutanix

Após conectar-se ao **Nutanix Prism**, crie VMs no cluster Nutanix.

Se a VM precisar de acesso à Internet

1. Vá para o console da AWS.
2. Crie uma nova sub-rede 10.0.130.0/24 na mesma VPC que a criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas desta sub-rede para direcionar todo o tráfego não local para o gateway NAT acima.

4. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
5. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a mesma sub-rede 10.0.130.0/24 usada na AWS.
6. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa nova sub-rede.

Se a VM não precisar de acesso à Internet

1. 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 nova 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.

> **Nota:**

> Para ver a opção para Nutanix no Web Studio, todas as VMs do conector devem ter o plug-in nutanix instalado, mesmo que não sejam usadas na zona nutanix.

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 a criação do site.

> Os componentes principais são o Citrix Delivery Controller™, Citrix Studio, Citrix Director e Citrix License Server.

(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

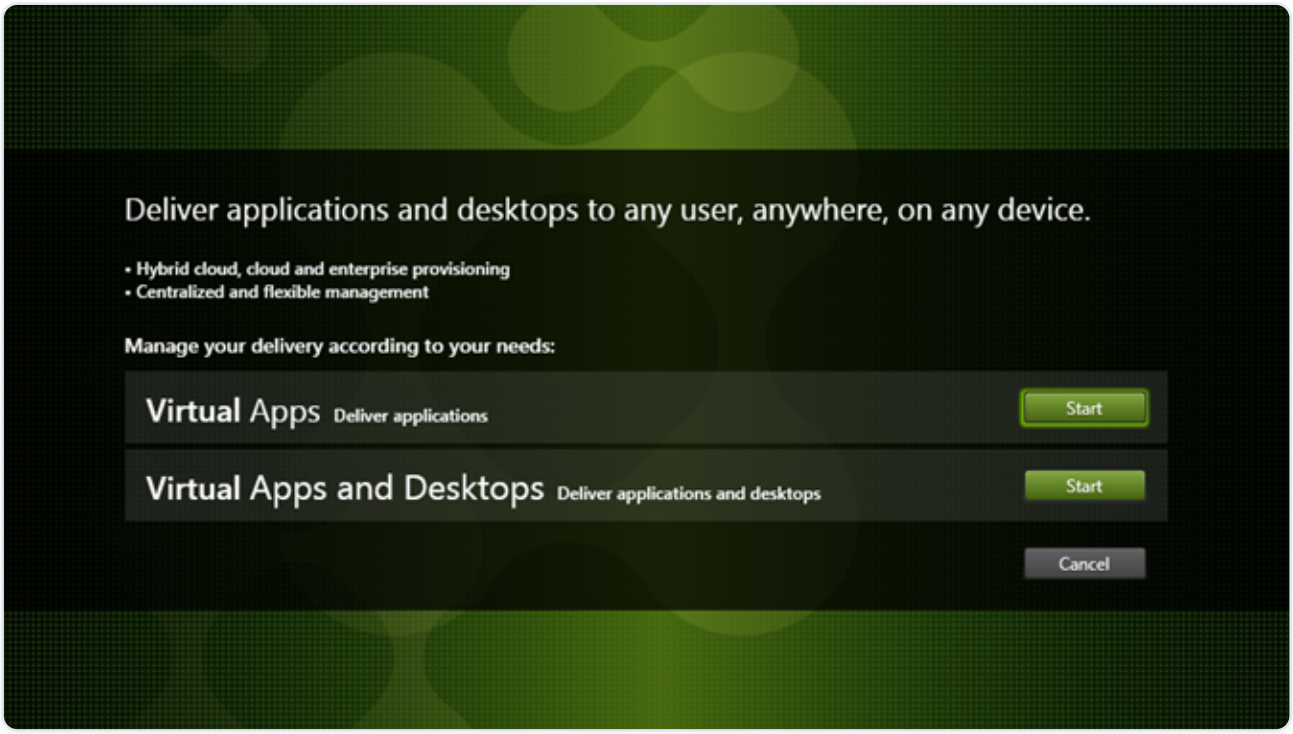
Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.

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 é instalado se a opção for omitida.

Etapa 3. Escolha o que instalar

Página de seleção de componentes no instalador de componentes(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/what-to-install-2.png)

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

Página do contrato de licença no instalador de componentes(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/core-license-75.png)

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

Página de componentes principais no instalador de componentes(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/core-components-75.png)

Na página **Componentes principais**:

- **Local:** Por padrão, os componentes são instalados em `C:\Program Files\Citrix`. O padrão é adequado para a maioria das implantações. Se você especificar um local diferente, ele deverá ter permissões de execução para o serviço de rede.
- **Componentes:** Por padrão, as caixas de seleção 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, o StoreFront e o License Server em servidores separados.

> **Nota:**
>
> Se você estiver instalando componentes em mais de um servidor, instale primeiro o Citrix License Server e as licenças, antes de instalar outros componentes em outros servidores. Para obter orientação, consulte a seção Instalação automática do Guia de Licenciamento para Citrix Virtual Apps and Desktops.
>
> Um ícone o alerta quando você opta por não instalar um componente principal obrigatório nesta máquina. Esse alerta o lembra de instalar esse componente, embora não necessariamente nesta máquina.

Clique em **Avançar**.

Opções de linha de comando: `/installdir`, `/components`, `/exclude`

Verificação de hardware

Ao instalar ou atualizar um Delivery Controller, o hardware é verificado. O instalador o alerta se a máquina tiver menos 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.

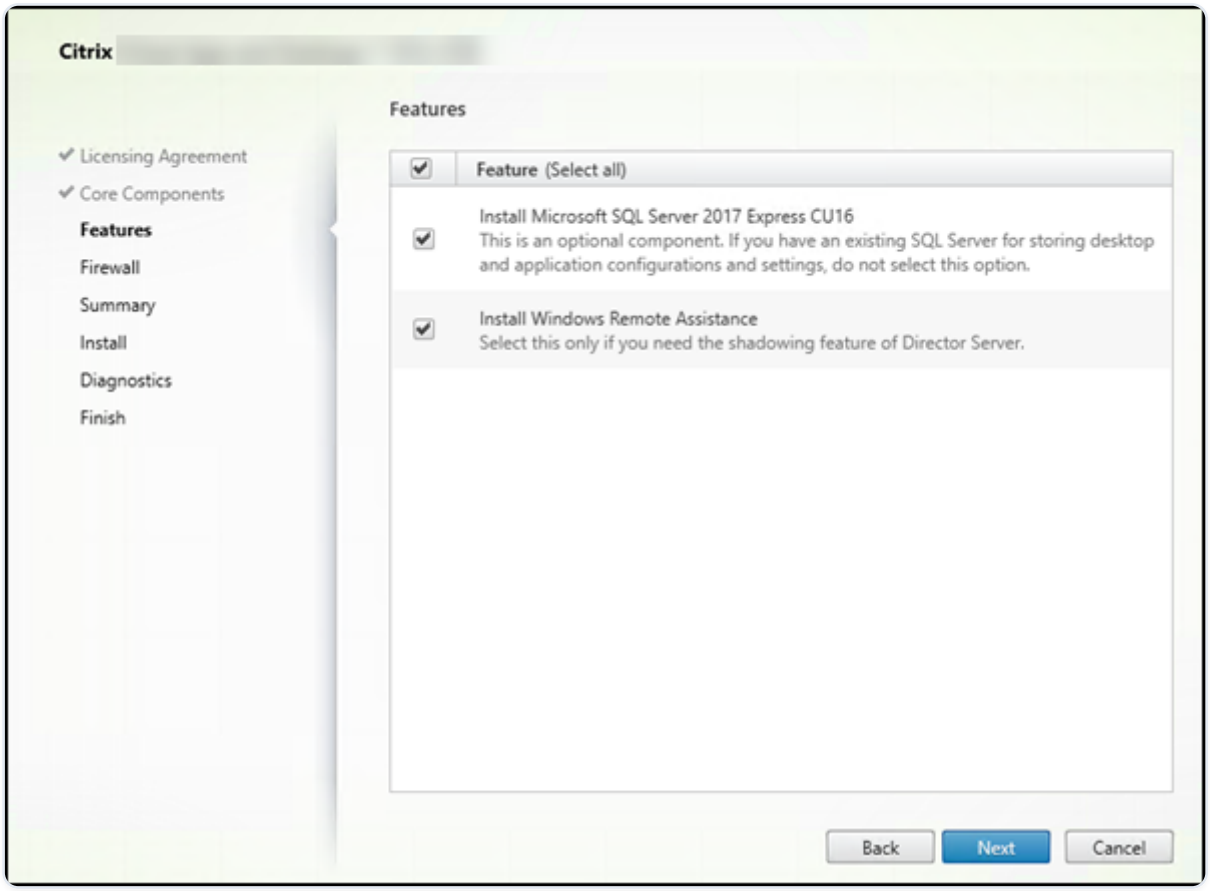
- Recomendado: Clique em **Cancelar** para interromper a instalação. Adicione mais RAM à máquina e inicie a instalação novamente.
- Alternativamente, clique em **Avançar** para continuar com a instalação. O site pode apresentar problemas de estabilidade.

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.
- Como alternativa, 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



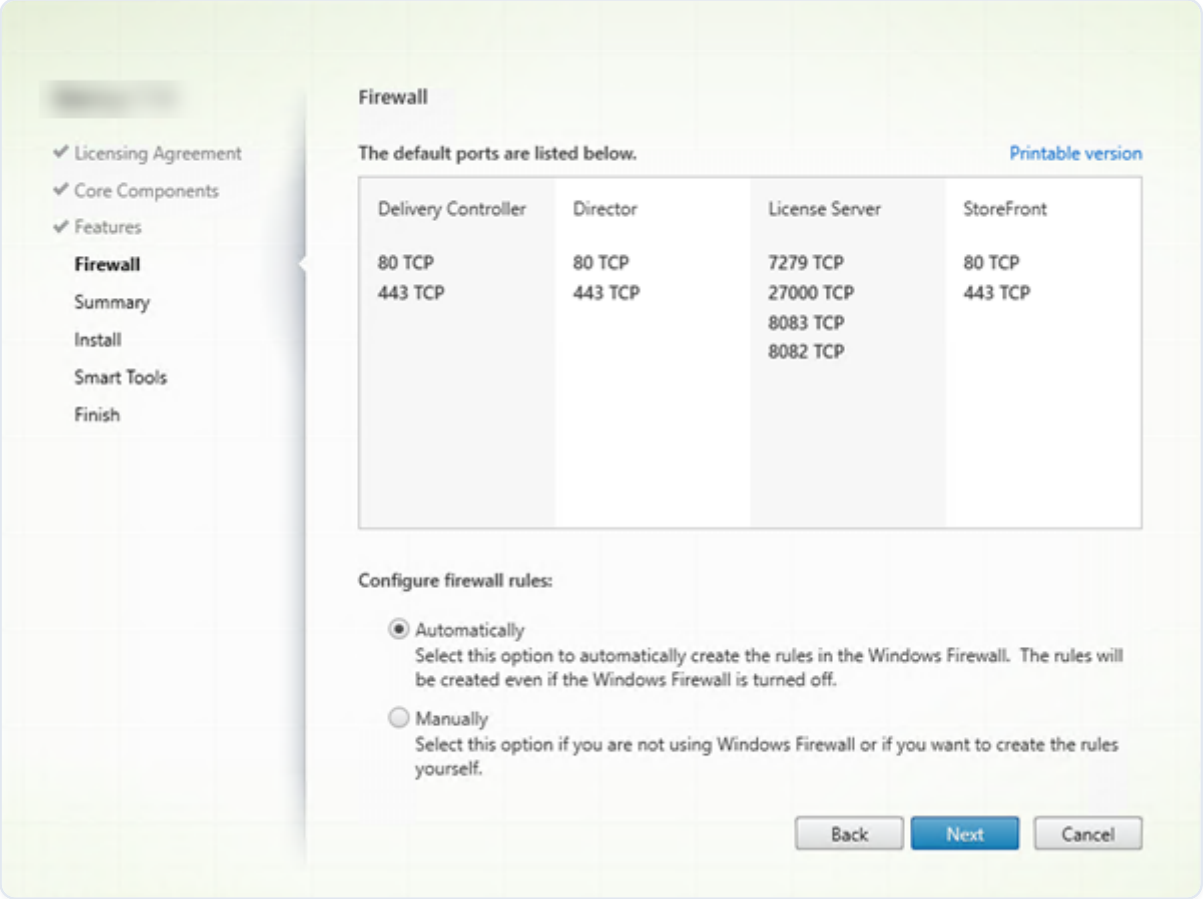
Na página **Recursos**:

- Escolha se deseja instalar o Microsoft SQL Server Express para usar como banco de dados do site. Por padrão, esta seleção está habilitada. Se você não estiver familiarizado com os bancos de dados do Citrix Virtual Apps and Desktops, revise Bancos de dados.
- Ao instalar o Director, o Assistência Remota do Windows é instalado automaticamente. Você escolhe se deseja habilitar o sombreamento no Assistência Remota do Windows para uso com o sombreamento de usuário do Director. A habilitação do sombreamento abre a porta TCP 3389. Por padrão, esse recurso está habilitado. A configuração padrão é adequada para a maioria das implantações. Esse recurso aparece apenas quando você está instalando o Director.

Clique em **Avançar**.

Opções de linha de comando: `/nosql` (para evitar a instalação), `/no_remote_assistance` (para evitar a habilitação)

Etapa 7. Abrir portas do firewall do Windows



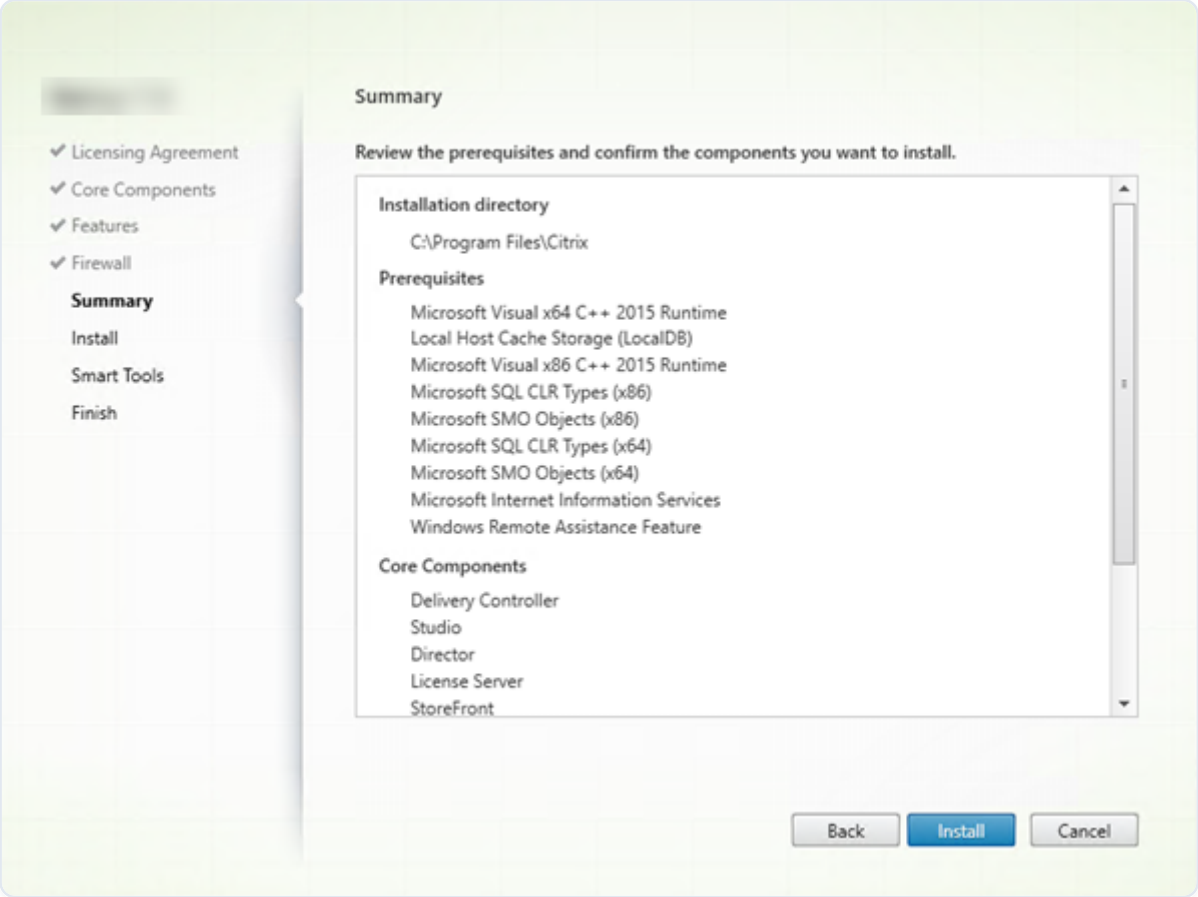
Por padrão, as portas na página **Firewall** são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja habilitado. A configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

(O gráfico mostra as listas de portas quando você instala todos os componentes principais nesta máquina. Esse tipo de instalação é geralmente apenas para implantações de teste.)

Opção de linha de comando: `/configure_firewall`

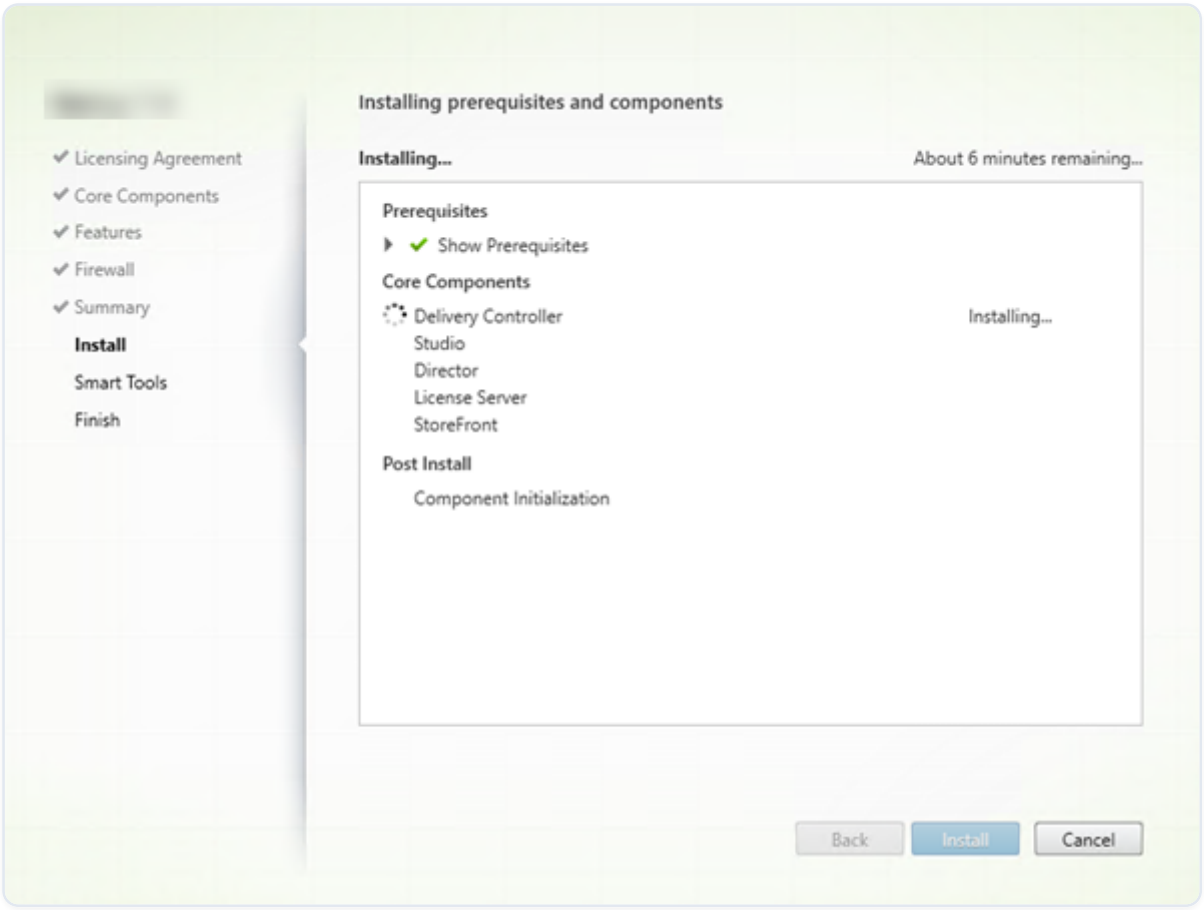
Etapa 8. Revisar pré-requisitos e confirmar a instalação



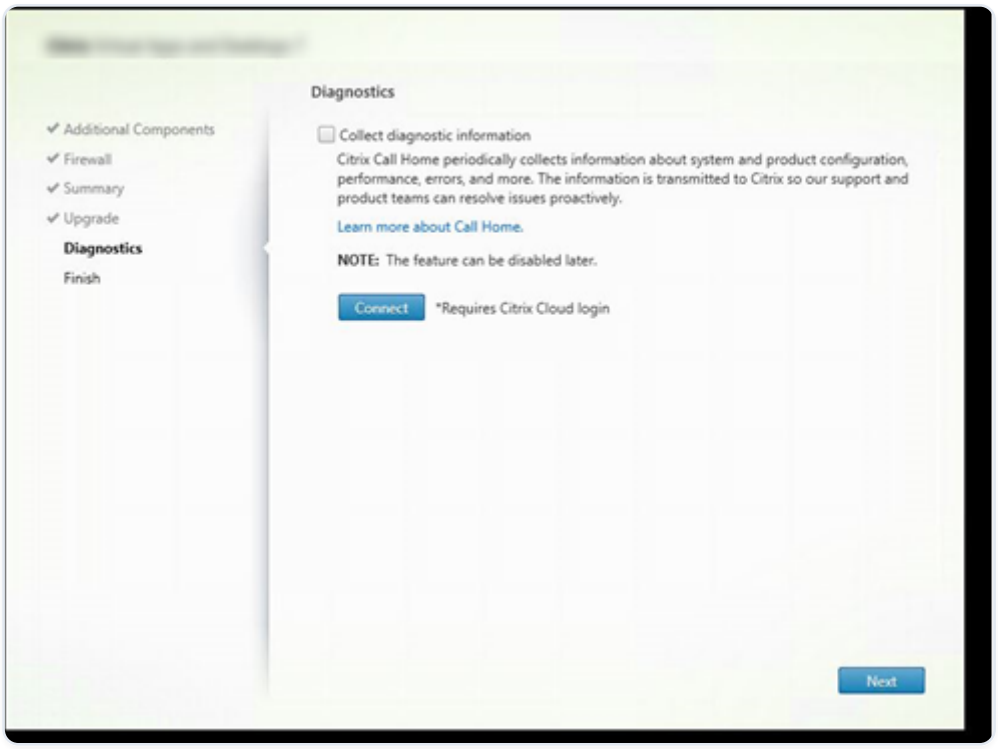
A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções, se necessário.

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

A exibição mostra o progresso da instalação:



Etapa 9. Diagnóstico



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 habilitado ou se o instalador encontrar um erro relacionado ao Citrix Telemetry Service.

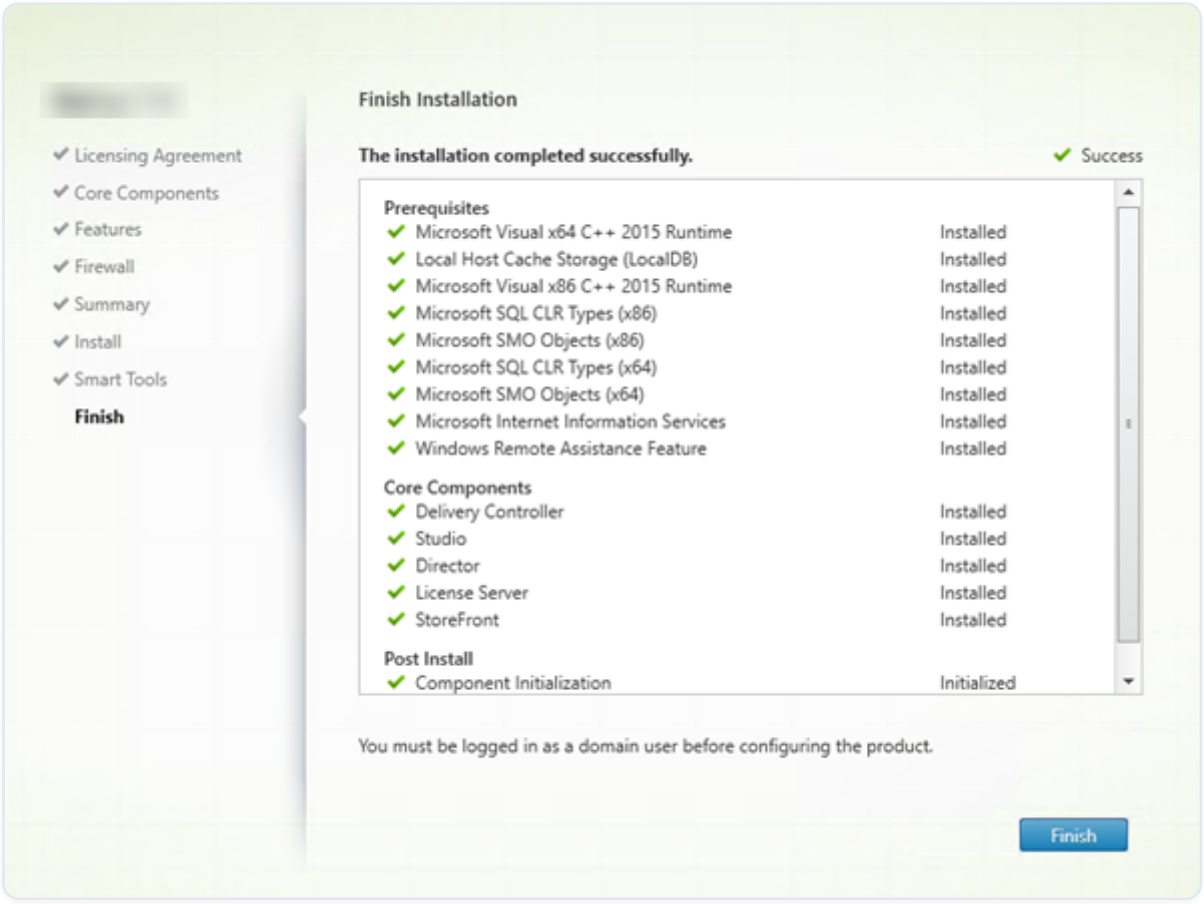
Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix. Você pode alterar sua escolha de inscrição mais tarde, após a instalação.

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 Citrix Insight Services**, 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. 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 11. Instalar os componentes principais restantes em outras máquinas

Se você instalou todos os componentes principais em uma máquina, continue com Próximas etapas. Caso contrário, execute o instalador em outras máquinas para instalar outros componentes. Você também pode instalar mais Controllers em outros servidores.

Próximas etapas

Depois de instalar todos os componentes necessários, use o Studio para criar um site.

Após criar o site, instale os VDAs.

A qualquer momento, você pode usar o instalador completo do produto para estender sua implantação com os seguintes componentes:

- **Componente de servidor do Universal Print Server:** Inicie o instalador no seu servidor de impressão.

a. Selecione **Universal Print Server** na seção **Estender Implantação**.

b. Aceite o contrato de licença.

c. Na página **Firewall**, por padrão, as portas TCP 7229 e 8080 são abertas no firewall se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Você pode desativar essa ação padrão se quiser abrir as portas manualmente.

Para instalar este componente a partir da linha de comando, consulte Opções de linha de comando para instalar um Universal Print Server.

- Serviço de Autenticação Federada.
- Gravação de Sessão.

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.

> 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 do Linux Virtual Delivery Agent.)

Antes de iniciar uma instalação, revise Preparar para instalar e conclua todas as tarefas de preparação.

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

Este artigo descreve a sequência do assistente de instalação ao instalar um VDA. Equivalentes de linha de comando são fornecidos. Para obter detalhes, consulte Instalar usando a linha de comando.

Etapa 1. Baixe o software do produto e inicie o assistente

Se você estiver usando o instalador completo do produto:

1. Se você ainda não baixou a ISO do produto:

- Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.
- Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.

2. Use uma conta de administrador local na imagem ou máquina onde você está instalando o VDA. Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não iniciar automaticamente, clique duas vezes no aplicativo **AutoSelect** ou na unidade montada.

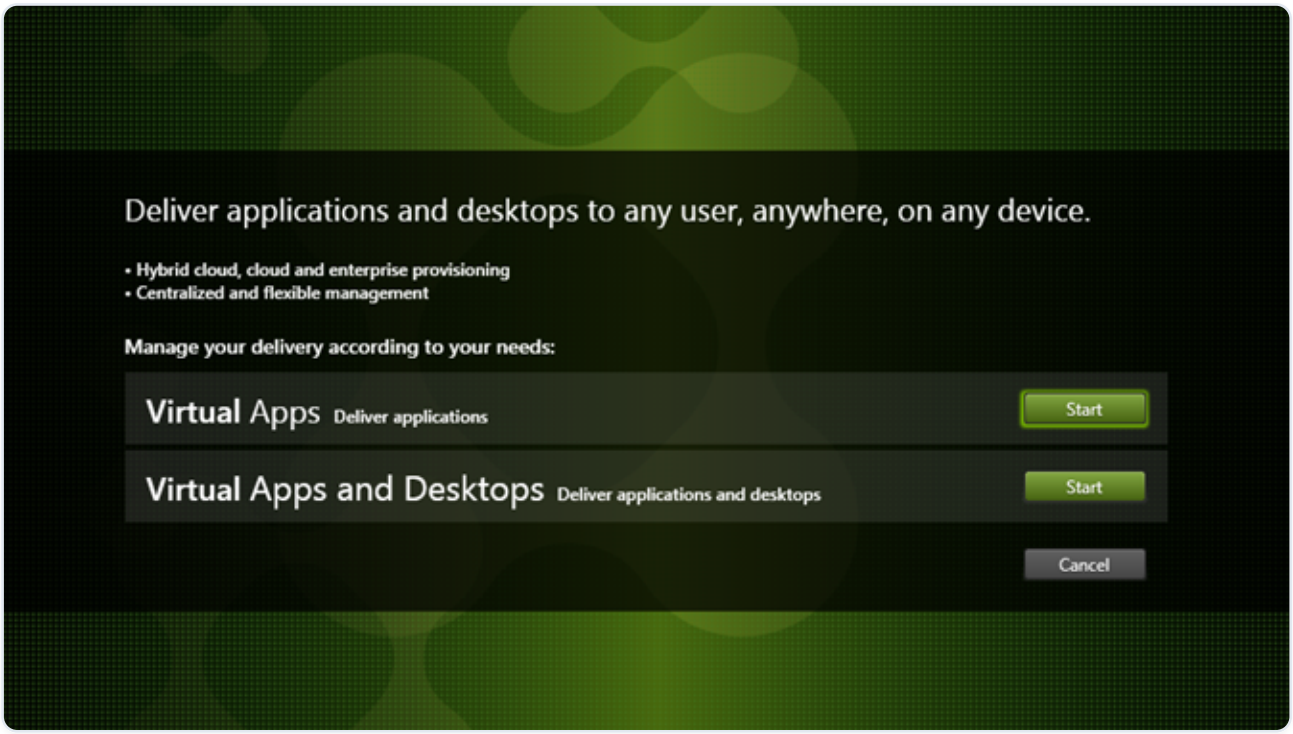
   O assistente de instalação é iniciado.

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.exe`: VDA de SO multi-sessão *versão*
   - `VDAWorkstationSetup.exe`: VDA de SO de sessão única *versão*
   - `VDAWorkstationCoreSetup.exe`: VDA de Serviços Principais de SO de sessão única *versão*
2. Clique com o botão direito do mouse no pacote e escolha **Executar como administrador.**

   O assistente de instalação é iniciado.

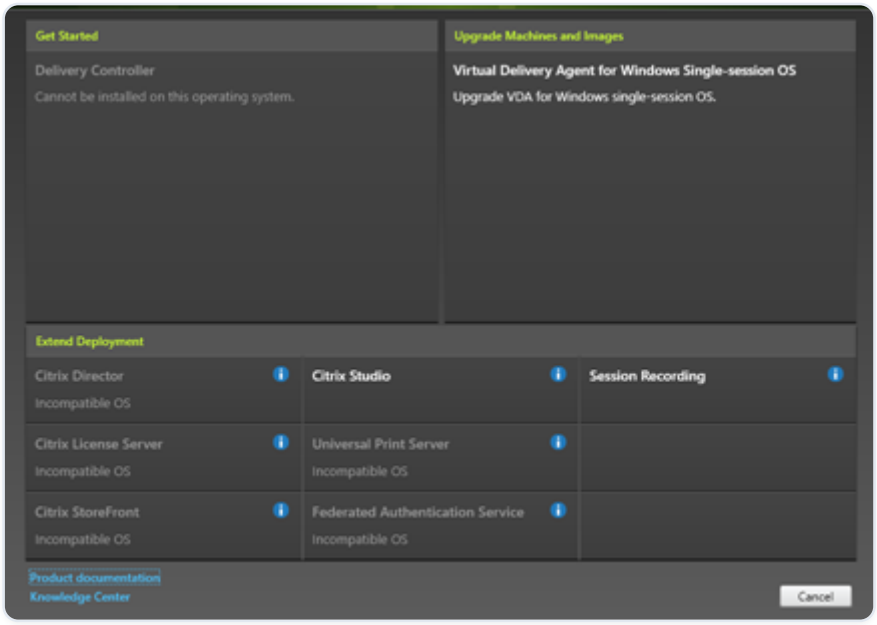
Etapa 2. Escolha qual produto instalar



Clique em **Iniciar** ao lado do produto a ser instalado: Citrix Virtual Apps ou Citrix Virtual Desktops. (Se a máquina já tiver um componente Citrix Virtual Apps ou Citrix Virtual Desktops instalado, esta página não aparecerá.)

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

Etapa 3. Selecione o VDA

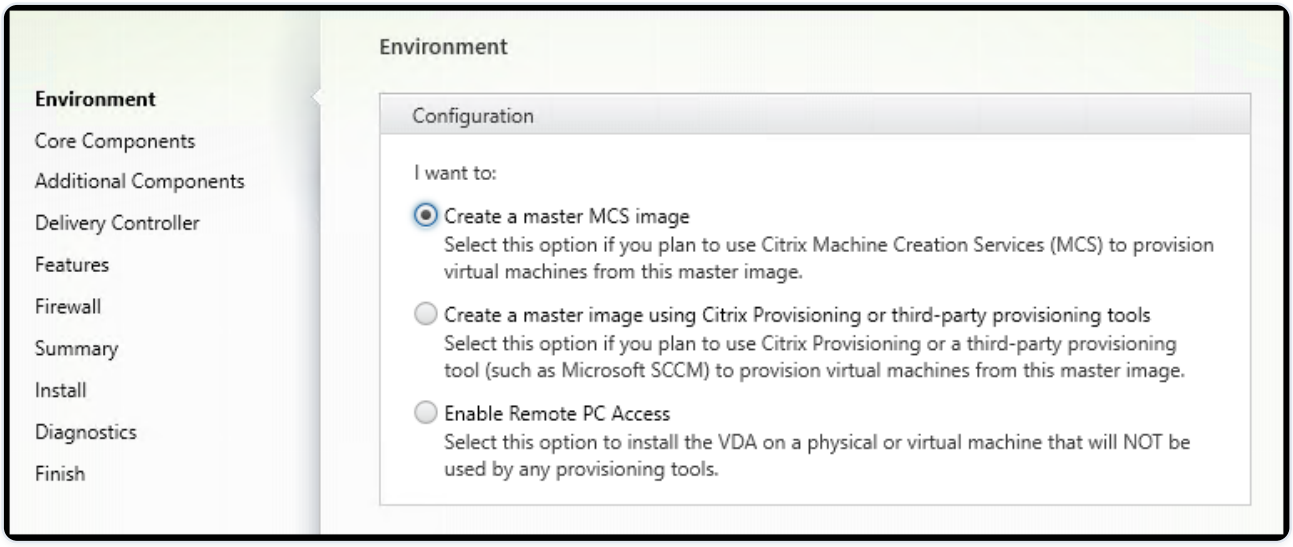


Selecione a entrada **Virtual Delivery Agent**. O instalador sabe se está sendo executado em um SO de sessão única ou multi-sessão, portanto, oferece apenas o tipo de VDA apropriado.

Por exemplo, ao executar o instalador em uma máquina Windows Server 2016, a opção VDA para SO multi-sessão está disponível. A opção VDA para SO de sessão única não é oferecida.

Se você tentar instalar (ou atualizar para) um VDA do Windows em um SO que não é 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 usará esta máquina como uma imagem para provisionar mais máquinas.

A opção que você escolher afeta quais ferramentas de provisionamento Citrix™ são instaladas automaticamente (se houver) e os valores padrão na página Componentes Adicionais do instalador do VDA.

Vários MSIs (de provisionamento e outros) são instalados automaticamente quando você instala um VDA. A única maneira de evitar a instalação deles 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 Serviço de Identidade da Máquina. 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 o Citrix Provisioning ou ferramentas de provisionamento de terceiros:** Selecione esta opção para instalar um VDA em uma imagem

de VM, se você planeja usar o Citrix Provisioning ou ferramentas de provisionamento de terceiros (como o Microsoft System Center Configuration Manager) para provisionar VMs.

Opção de linha de comando: `/masterpvsimage`

- (Aparece apenas em máquinas de SO multi-sessão) **Habilitar conexões intermediadas a um servidor:** Selecione esta opção para instalar um VDA em uma máquina física ou virtual que não é usada como imagem para provisionar outras máquinas.

  Opção de linha de comando: `/remotepc`

- (Aparece apenas em máquinas de SO 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.

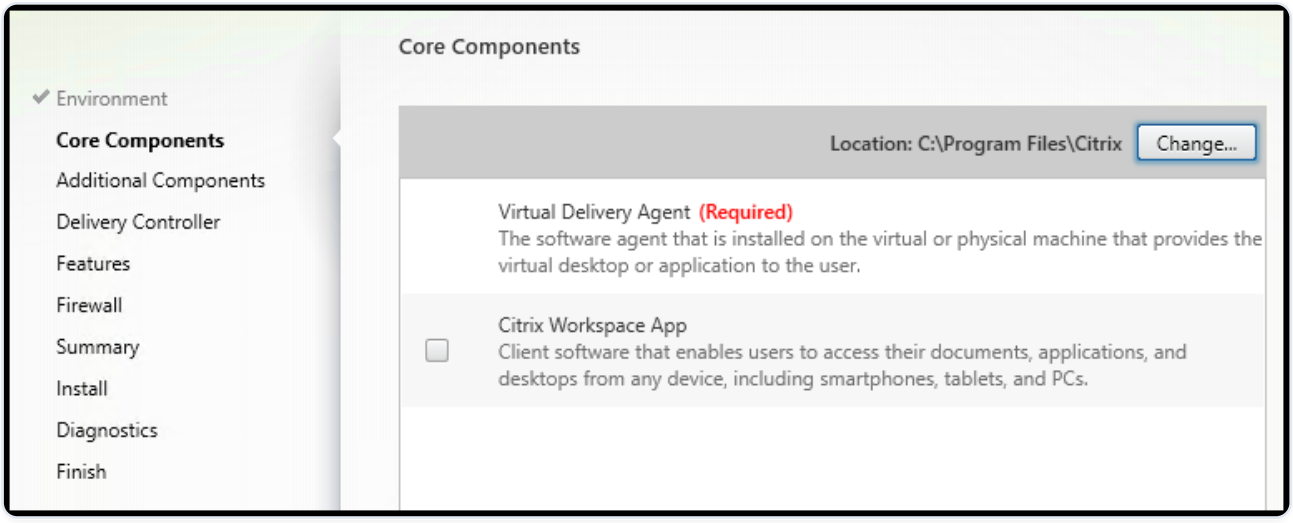
  Opção de linha de comando: `/remotepc`

Clique em **Avançar**.

Esta página não aparece:

- Se você estiver atualizando um VDA
- Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`

Etapa 5. Selecione os componentes a serem instalados e o local de instalação



Na página **Componentes principais**:

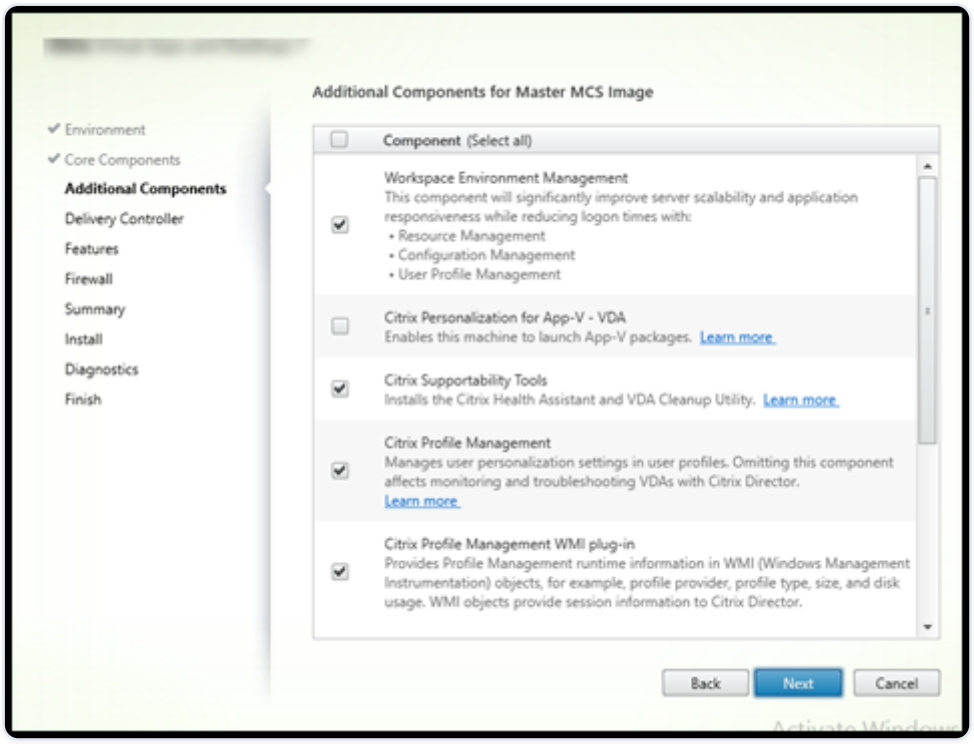
- **Local:** Por padrão, os componentes são instalados em `C:\Program Files\Citrix`. Esse padrão é adequado para a maioria das implantações. Se você especificar um local diferente, esse local deverá ter permissões de execução para o serviço de rede.

- **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

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 DE COMPONENTES ADICIONAIS	PÁGINA AMBIENTE: "IMAGEM MESTRE COM MCS" OU "IMAGEM MESTRE COM CITRIX PROVISIONING" SELECIONADA	PÁGINA AMBIENTE: "HABILITAR CONEXÕES INTERMEDIADAS AO SERVIDOR" (PARA SO MULTI-SESSÃO) OU "ACESSO REMOTO PARA PC" (PARA SO DE SESSÃO ÚNICA) SELECIONADO
Workspace Environment Management™	Não selecionado	Não selecionado
Personalização Citrix para App-V	Não selecionado	Não selecionado
Camada de Personalização do Usuário	Não selecionado	Não exibido porque não é válido para este caso de uso.
Ferramentas de Suporte Citrix	Selecionado	Não selecionado
Citrix Profile Management	Selecionado	Não selecionado
Citrix Profile Management WMI Plug-in	Selecionado	Não selecionado
Citrix VDA Upgrade Agent	Não selecionado	Não selecionado
Citrix Files para Windows	Não selecionado	Não selecionado
Citrix Files para Outlook	Não selecionado	Não selecionado
Cache de gravação MCSIO para otimização de armazenamento	Não selecionado	Não selecionado
Configuração do protocolo Rendezvous	Não selecionado	Não selecionado

Esta página não aparece se:

- Você está usando o `VDAWorkstationCoreSetup.exe` instalador. 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.)

- **Workspace Environment Management:** Instale este componente se sua implantação usar o Citrix Workspace Environment Management. Para obter detalhes, consulte Workspace Environment Management.

  Opções de linha de comando: `/includeadditional "Citrix WEM Agent"` para habilitar a instalação do componente, `/exclude "Citrix WEM Agent"` para impedir a instalação do componente

- **Personalização Citrix para App-V:** Instale este componente se você usar aplicativos de pacotes Microsoft App-V. Para obter detalhes, consulte App-V.

  Opção de linha de comando: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar a instalação do componente, `/exclude "Citrix Personalization for App-V – VDA"` para impedir a instalação do componente

- **Camada de Personalização de Usuário Citrix:** Instala o MSI para a camada de personalização do usuário. Para obter detalhes, consulte Camada de personalização do usuário.

  Este componente aparece apenas ao instalar um VDA em uma máquina Windows 10 de sessão única.

  Opção de linha de comando: `/includeadditional "User Personalization Layer"` para habilitar a instalação do componente, `/exclude "User Personalization Layer"` para impedir a instalação do componente

- **Ferramentas de Suporte Citrix** Instala o MSI que contém ferramentas de suporte Citrix, como o Citrix Health Assistant.

  Opção de linha de comando: `/includeadditional "Citrix Supportability Tools"` para habilitar a instalação do componente, `/exclude "Citrix Supportability Tools"` 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 **Detalhes do usuário** e **Ponto de extremidade**, o painel **Personalização** e o painel **Duração do logon** falham. Nas páginas **Painel** e **Tendências**, o painel **Duração média do logon** exibe dados apenas para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Serviço Citrix Profile Management. A ativação 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 Plugin"` para habilitar a instalação do componente, `/exclude "Citrix Profile Management WMI Plugin"` 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

- **Citrix Files para Windows:** Este componente permite que os usuários se conectem à sua conta do Citrix Files. Eles podem então interagir com o Citrix Files através de uma unidade mapeada no sistema de arquivos do Windows (sem exigir uma sincronização completa de seu conteúdo). Para obter mais informações, consulte Content Collaboration.

Opções de linha de comando: `/includeadditional "Citrix Files for Windows"` para habilitar a instalação do componente, `/exclude "Citrix Files for Windows"` para impedir a instalação do componente

- **Citrix Files para Outlook:** O Citrix Files para Outlook permite que você ignore as restrições de tamanho de arquivo e adicione segurança aos seus anexos ou e-mails, enviando-os através do Citrix Files. Você pode fornecer uma solicitação de upload de arquivo seguro para colegas de trabalho, clientes e parceiros diretamente em seu e-mail. Para obter mais informações, consulte Content Collaboration.

  Opções de linha de comando: `/includeadditional "Citrix Files for Outlook"` para habilitar a instalação do componente, `/exclude "Citrix Files for Outlook"` para impedir a instalação do componente

- **Cache de gravação MCSIO para otimização de armazenamento:** Instala o driver Citrix MCS IO. Para obter mais informações, consulte Armazenamento compartilhado por hipervisores e Configurar cache para dados temporários.

  Opções de linha de comando: `/includeadditional "Citrix MCS IODriver"` para habilitar a instalação do componente, `/exclude "Citrix MCS IODriver"` para impedir a instalação do componente

- **Configuração de Proxy Rendezvous:** Instale este componente se você planeja usar o protocolo Rendezvous com o Citrix Gateway Service em seu ambiente e tiver um proxy não transparente em sua rede para conexões de saída. Apenas proxies HTTP são suportados.

  Se você instalar este componente, especifique o endereço do proxy ou o caminho do arquivo PAC na página **Configuração de Proxy Rendezvous**. Para obter detalhes do recurso, consulte protocolo Rendezvous.

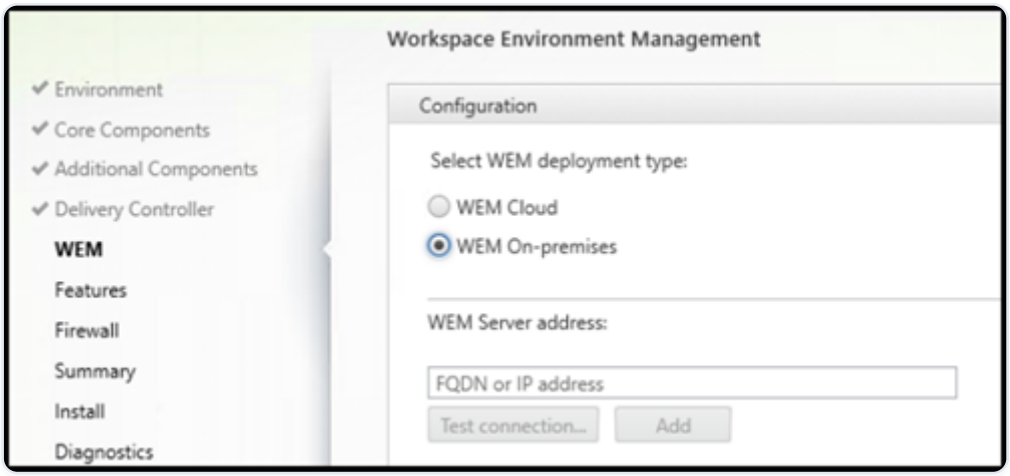
  Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para habilitar a instalação do componente, `/exclude "Citrix Rendezvous V2"` para impedir a instalação do componente

Etapa 7. Gerenciamento do Ambiente de Trabalho

A página **Workspace Environment Management** (WEM) aparece apenas quando você habilita a caixa de seleção correspondente na página **Componentes Adicionais**.

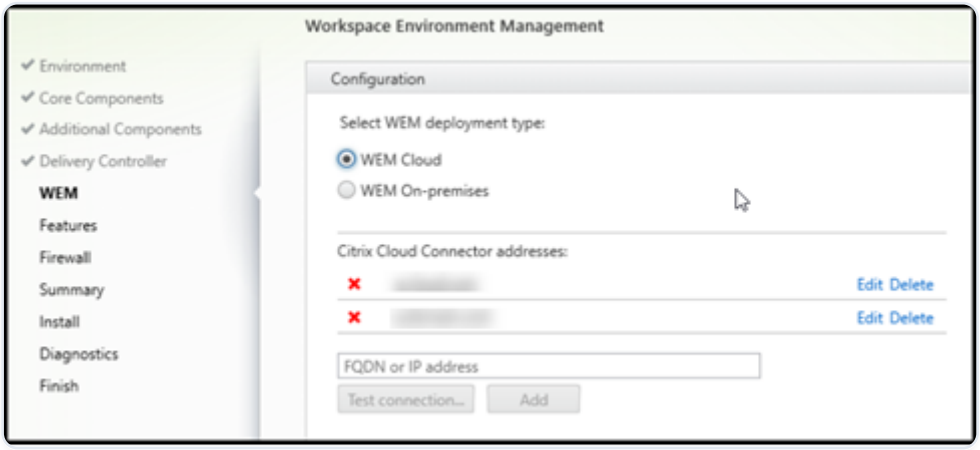
1. Selecione se você tem uma implantação WEM local ou WEM na nuvem (serviço).
2. Adicione um FQDN ou endereço IP. Caracteres especiais são ignorados.

- Para WEM local: Endereço do Servidor de Infraestrutura WEM



> **Observação:**
>
> Você pode ver a seguinte mensagem de erro ao testar uma conexão de servidor WEM: `Unable to establish connection with "<the address you entered>"`. Se o endereço estiver correto e o servidor puder ser contatado, você pode ignorar a mensagem.

- Para o serviço WEM: Endereço do Cloud Connector

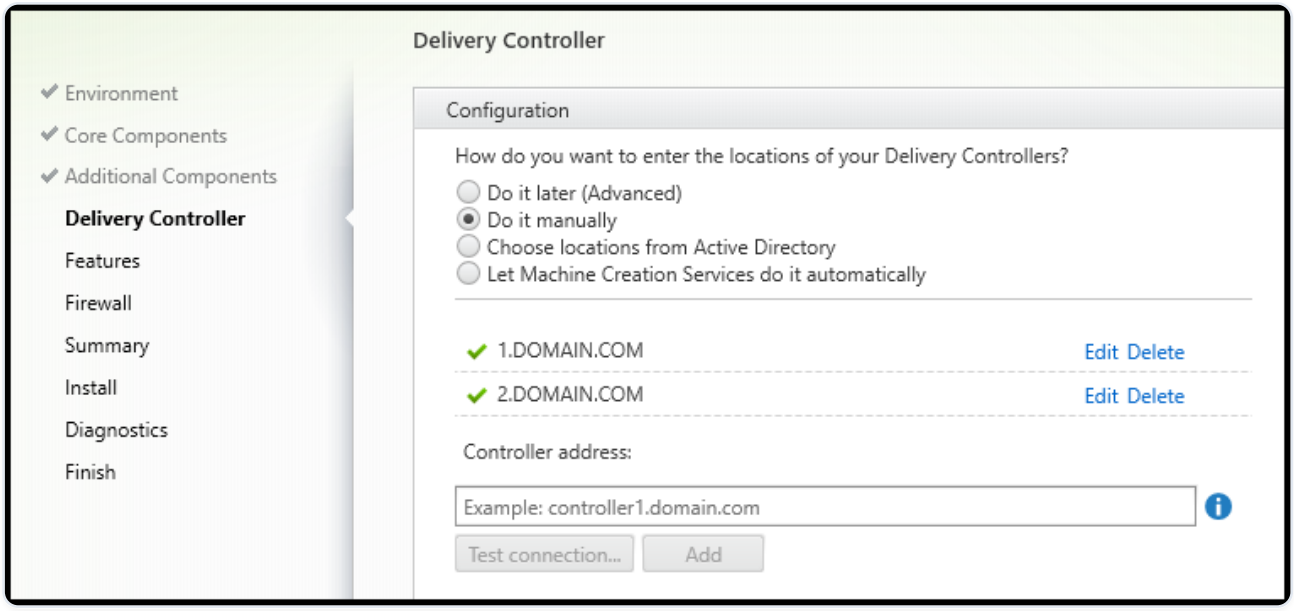


3. Clique em **Testar Conexão**. A porta deve estar aberta no firewall.
4. Após um teste de conexão bem-sucedido, clique em **Adicionar**.
5. Para uma implantação de serviço WEM, repita os passos 2-4 para outros Cloud Connectors.
6. Clique em **Avançar**.

Opções de linha de comando: `/wem_server`, `/wem_cloud_connectors`

Mais opções de configuração do agente WEM estão disponíveis na interface de linha de comando. Consulte opções de instalação de linha de comando.

Passo 8. 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 o que deseja fazer antes de continuar. Para especificar endereços mais tarde, você pode executar novamente o instalador ou usar a Política de Grupo da Citrix. O assistente também o lembrará na página **Resumo**.
- **Escolher locais do Active Directory:** Válido somente quando a máquina está ingressada em um domínio e o usuário é um usuário de domínio.
- **Deixar o Machine Creation Services fazer isso automaticamente:** Válido somente ao usar o MCS para provisionar máquinas.

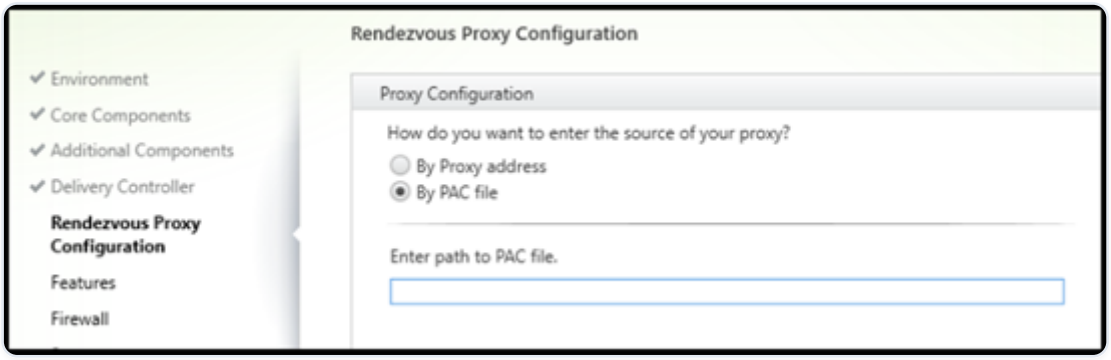
Clique em **Avançar**. Se você selecionou **Fazer mais tarde (Avançado)**, será solicitado que você confirme que especificará os endereços do Controller mais tarde.

Outras considerações:

- O endereço não pode conter caracteres não alfanuméricos.
- Se você especificar endereços durante a instalação do VDA e na Política de Grupo, as configurações da política substituirão as configurações fornecidas durante a instalação.
- O registro bem-sucedido do VDA requer 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 9. Configuração do Proxy Rendezvous



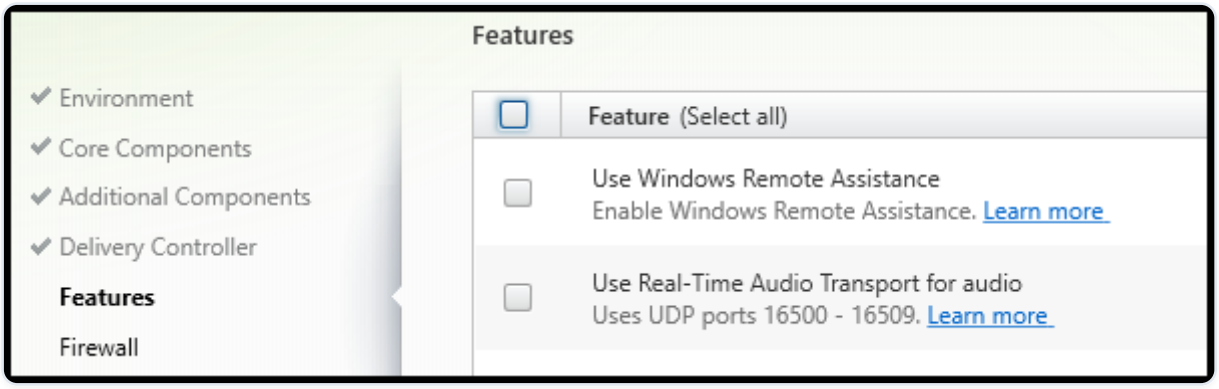
A página **Configuração do Proxy Rendezvous** aparece somente se você ativou a caixa de seleção **Configuração do Proxy Rendezvous** na página **Componentes Adicionais**.

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 proxy deve estar aberto para que o teste de conexão seja bem-sucedido. Se uma conexão não puder ser feita com o proxy, você pode escolher se deseja continuar com a instalação do VDA.

Opção de linha de comando: `/proxyconfig`

Etapa 10. 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 a voz sobre IP for amplamente utilizada 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 o Citrix DaaS (Padrão = desabilitado).

  Opção de linha de comando: `/xendesktopcloud`

Se esta página contiver um recurso chamado **MCS I/O**, não o utilize. O recurso MCS IO é configurado na página **Componentes Adicionais**.

Clique em **Avançar**.

Etapa 11. Portas do firewall

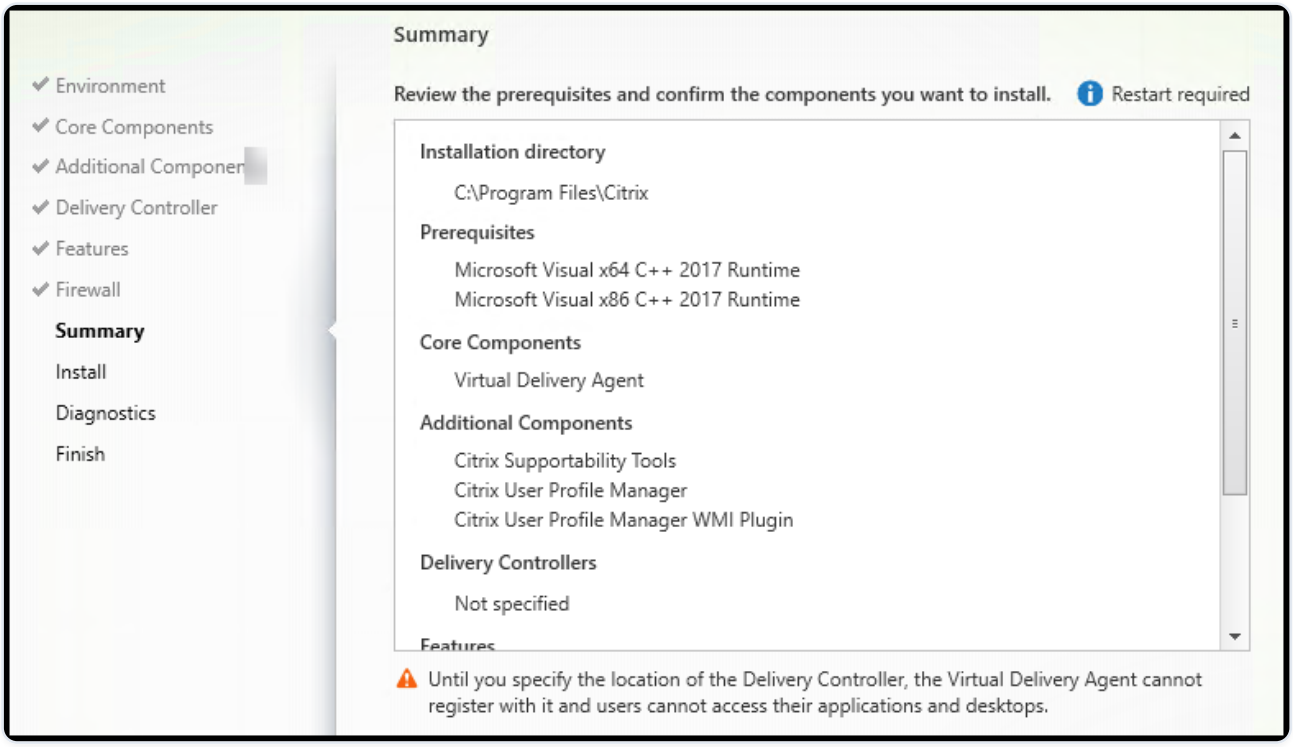


Na página **Firewall**, por padrão, as portas são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Essa configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

Opção de linha de comando: `/enable_hdx_ports`

Etapa 12. Revisar pré-requisitos e confirmar a instalação



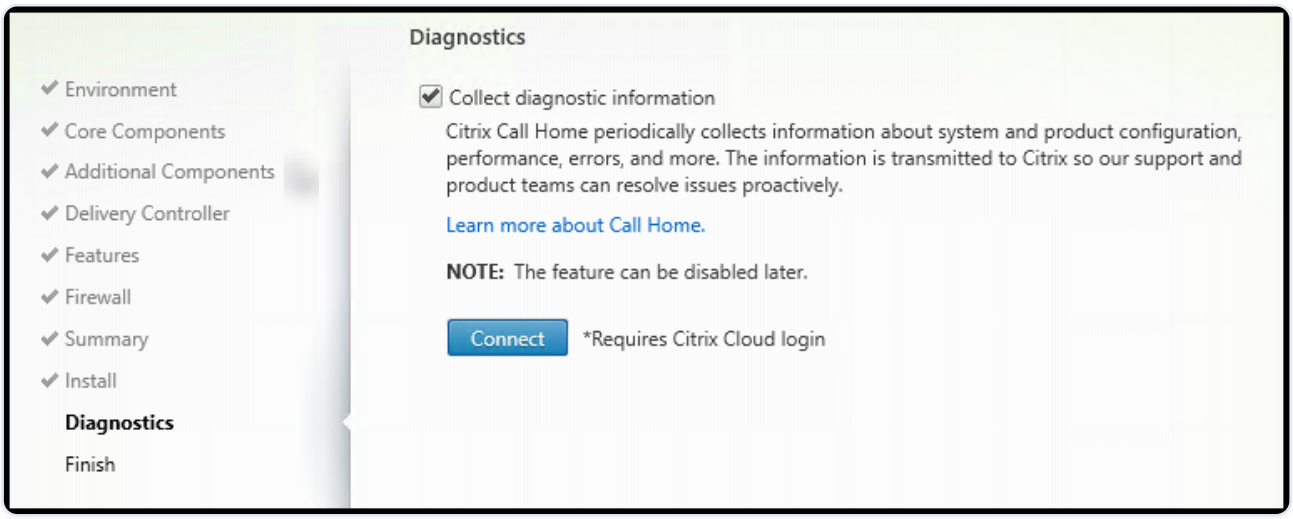
A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções.

(Somente VDAs de sessão única) Marque a caixa de seleção **Habilitar restauração automática se a atualização falhar** para ativar o recurso de restauração em caso de falha. Para obter detalhes, consulte Restaurar em caso de falha de instalação ou atualização.

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

Se os pré-requisitos ainda não estiverem instalados ou ativados, a máquina poderá reiniciar uma ou mais vezes. Consulte Preparar para instalar.

Etapa 13. Diagnóstico



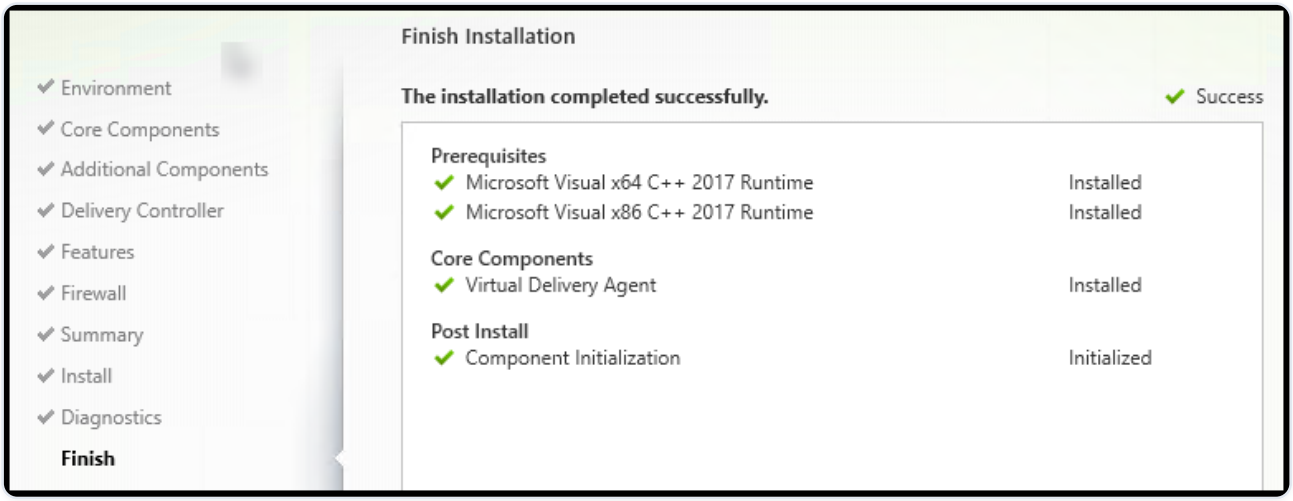
Na página **Diagnóstico**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix.

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

Ao usar o instalador completo do produto, se você clicar em **Conectar** na página **Diagnóstico** sem primeiro selecionar **Coletar informações de diagnóstico**, depois de fechar a caixa de diálogo **Conectar aos Serviços Citrix Insight**, o botão **Avançar** é 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 14. Conclua esta instalação



A página **Concluir** contém marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com sucesso.

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

Próximas etapas

Repita o procedimento acima para instalar VDAs em outras máquinas ou imagens, se necessário.

Depois de instalar todos os VDAs, inicie o Studio. Se você ainda não criou um site, o Studio o guiará automaticamente para essa tarefa. Depois disso, o Studio o guiará para criar um catálogo de máquinas e, em seguida, um grupo de entrega. Consulte:

- Criar um site
- Criar catálogos de máquinas
- Criar grupos de entrega

Citrix Optimizer

O Citrix Optimizer é uma ferramenta para o sistema operacional Windows que ajuda os administradores Citrix a otimizar VDAs removendo e otimizando vários componentes.

Após instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Consulte CTX224676. O artigo CTX contém o pacote de download, além de instruções sobre como instalar e usar o Citrix Optimizer.

Personalizar um VDA

Para personalizar um VDA instalado:

1. No recurso do Windows para remover ou alterar programas, selecione **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Em seguida, clique com o botão direito e selecione **Alterar**.
2. Selecione **Personalizar Configurações do Virtual Delivery Agent**. Quando o instalador for iniciado, você poderá alterar:
   - Endereços do Controller
   - Porta TCP/IP para registrar com o Controller (padrão = 80)
   - Abrir as portas do Firewall do Windows automaticamente

Solucionar problemas

- 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 Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou uma área de trabalho aos usuários até que ele se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

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.

Introdução

Este artigo se aplica à instalação de componentes em máquinas com sistemas operacionais Windows. Para obter informações sobre VDAs para sistemas operacionais Linux, consulte Agentes de Entrega Virtual Linux.

Este artigo descreve como emitir comandos de instalação do produto. Antes de iniciar qualquer instalação, revise Preparar para instalar. Esse artigo inclui descrições dos instaladores disponíveis.

Para ver o progresso da execução do comando e os valores de retorno, você deve ser o administrador original ou usar **Executar como administrador**. Para obter mais informações, consulte a documentação de comando da Microsoft.

Como complemento ao uso direto dos comandos de instalação, scripts de exemplo são fornecidos no ISO do produto que instalam, atualizam ou removem VDAs em máquinas no Active Directory. Para obter detalhes, consulte Instalar VDAs usando scripts.

Se você tentar instalar ou atualizar em uma versão do sistema operacional Windows que não é suportada para esta versão do Citrix Virtual Apps and Desktops, uma mensagem o guiará para informações sobre suas opções. Consulte Sistemas operacionais anteriores.

Para obter informações sobre como a Citrix relata o resultado 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.

Opções de linha de comando para instalar componentes principais

As seguintes opções são válidas ao instalar componentes principais com o comando `XenDesktopServerSetup.exe`. Para mais detalhes sobre as opções, consulte Instalar componentes principais.

> **Observação:**
>
> - Não use `/exclude` ao usar opções de linha de comando para instalar componentes principais.
> - Se você atualizar um componente usando `/components`, outros componentes também poderão ser atualizados. Isso é para evitar possíveis problemas de compatibilidade entre diferentes componentes.
> - Se você quiser atualizar apenas um componente, use o instalador individual desse componente. Consulte Atualizar uma implantação.

- **/components** *componente* ...

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

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server

  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 habilitado. 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 = falso

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_pending_reboot_check**

  Ao instalar ou atualizar componentes principais, impede a verificação de uma reinicialização pendente de uma instalação anterior do Windows na máquina.

- **/no_remote_assistance**

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

- **/semreinicialização**

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

- **/semretomar**

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

- **/sem-sql**

  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 é instalado para ser usado como o banco de dados do site.

  Esta opção não tem efeito na instalação do SQL Server Express LocalDB usado para o Cache do 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 é iniciada.

- **/remover**

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

- **/removertudo**

  Remove todos os componentes principais instalados.

- **/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 armazena arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

- **/XenApp**

  Instala o Citrix Virtual Apps. Se esta opção for omitida, o Citrix Virtual Apps and Desktops™ será instalado.

Exemplos de instalação de componentes principais

O comando a seguir instala um Delivery Controller™, Studio, Citrix Licensing e SQL Server Express em um servidor. As portas de firewall necessárias para as comunicações dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

O comando a seguir instala um Citrix Virtual Apps™ Controller, Studio e SQL Server Express no servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

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:
   - Virtual Delivery Agent de SO multissessão: `VDAServerSetup.exe`
   - Virtual Delivery Agent de SO de sessão única: `VDAWorkstationSetup.exe`
   - Virtual Delivery Agent de Serviços Principais de SO de sessão única: `VDAWorkstationCoreSetup.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 `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. O diretório deve existir. Caso contrário, a extração falhará. Em seguida, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

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

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

Se você está familiarizado com o instalador completo do produto:

- Execute o instalador autônomo `VDAServerSetup.exe` ou `VDAWorkstationSetup.exe` como se fosse o comando `XenDesktopVdaSetup.exe` em tudo, exceto no seu nome.
- O instalador `VDAWorkstationCoreSetup.exe` é diferente, porque 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.

- **/components** *componente*\[,*componente*\]

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

  - `VDA`: Agente de Entrega Virtual
  - `PLUGINS`: aplicativo Citrix Workspace™ para Windows

  Para instalar o VDA e o aplicativo Citrix Workspace para Windows, especifique `/components vda,plugins`.

  Se esta opção for omitida, apenas o VDA será instalado (não o aplicativo Citrix Workspace).

  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 Controladores separados por espaço com os quais o VDA pode se comunicar, entre aspas retas. Não especifique as opções `/site_guid` e `/controllers`.

- **/desabilitarmétricasdeexperiência**

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

- **/enable_hdx_ports**

  Abre as portas no firewall do Windows exigidas pelo VDA e pelos recursos habilitados (exceto Assistência Remota do Windows), se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

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

- **/enable_hdx_udp_ports**

Abre as portas UDP no firewall do Windows que o transporte adaptativo HDX usa, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

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

- **/enable_real_time_transport**

  Habilita ou desabilita o uso de UDP para pacotes de áudio (Transporte de Áudio em Tempo Real para áudio). Habilitar esse recurso pode melhorar o desempenho do áudio. Inclua a opção `/enable_hdx_ports` se você quiser que as portas UDP sejam abertas automaticamente quando o Serviço de Firewall do Windows for detectado.

- **/enable_remote_assistance**

  Habilita o recurso de sombreamento 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 retas. Por exemplo, instalar ou atualizar um VDA em uma imagem que não é gerenciada pelo MCS não requer o componente Machine Identity Service. Os valores válidos são os seguintes:

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA	SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Universal Print Client`
`Citrix Profile Management`	`Citrix Profile Management`	`Citrix Vda Log Capture Service`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`	`CSE Component`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`	`Director VDA Plug-in`
`Citrix Supportability Tools`	`Citrix Supportability Tools`	`Machine Management Provider`
`Citrix Telemetry Service`	`Citrix Telemetry Service`	`VDA Monitor Plug-in`
`Citrix Universal Print Client`	`Citrix Universal Print Client`	`VDA WMI Proxy Plug-in`
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA	SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`Citrix WEM Agent`	`Citrix WEM Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	

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.

- **/incluiradicional** "*componente*"\[,"*componente*"\]

  Inclui a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas retas. Esta opção pode ser útil ao criar uma implantação de Acesso Remoto para 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`
`Citrix Supportability Tools`	`Citrix Supportability Tools`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix WEM Agent`	`Citrix WEM Agent`
`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 Citrix Provisioning™ ou uma ferramenta de provisionamento de terceiros (como Microsoft System Center Configuration Manager) para provisionar VMs.

- **/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 falhará. A maioria das edições compatíveis do Windows já vem com o Media Foundation instalado, exceto as edições N.

- **/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 habilitação do recurso Experiência de Área de Trabalho Aprimorada. Este recurso também é controlado pela configuração de política Citrix de Experiência de Área de Trabalho Aprimorada.

- **/semreinicialização**

Impede uma reinicialização após a instalação. O VDA não pode ser usado antes de uma reinicialização.

- **/semretomar**

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

- **/númerodaporta** *porta*

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

- **/proxyconfig** "*endereço ou caminho do arquivo PAC*"

  Válido apenas se o comando contiver `/includeadditional "Citrix Rendezvous V2"`. O endereço ou caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para detalhes do recurso, consulte protocolo Rendezvous.

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

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

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

- **/reconfigurar**

  Personaliza as configurações do VDA configuradas anteriormente quando usado com as opções `/portnumber`, `/controllers` ou `/enable_hdx_ports`. Se você especificar esta opção sem também especificar a opção `/quiet`, a interface gráfica para personalizar o VDA será iniciada.

- **/pcremoto**

  Válido apenas para implantações de Acesso Remoto a PC (SO de sessão única) ou conexões intermediadas (SO de 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).

- **/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 multi-sessão compatível. Omita esta opção ao instalar um VDA para SO multi-sessão em uma máquina Windows multi-sessão.

  Antes de usar esta opção, consulte Server VDI.

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

- **local_guid** *guid*

  Identificador Globalmente Único da Unidade Organizacional (OU) do Active Directory do site. Isso associa uma área de trabalho virtual a um site quando você está usando o Active Directory para descoberta (a atualização automática é o método de descoberta recomendado e padrão). O GUID do site é uma propriedade do site exibida no Studio. Não especifique as opções `/site_guid` e `/controllers`.

- **dirtemp** *diretório*

Diretório para armazenar arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

Esta opção não está disponível na interface gráfica.

- **máquinavirtual**

  Válido apenas ao instalar um VDA em uma VM. Substitui a detecção pelo instalador de uma máquina física, onde as informações do BIOS passadas para as VMs as fazem parecer máquinas físicas.

  Esta opção não está disponível na interface gráfica.

- **/wem_add_firewall_rules**

  Adiciona regras de firewall do agente WEM.

- **/wem_agent_cache_location**

  Localização alternativa do cache do agente WEM.

- **/wem_agent_port**

  Porta que o agente WEM usa para se comunicar com o servidor de infraestrutura WEM.

- **/wem_cached_data_sync_port**

  Porta que o agente WEM usa para sincronizar o cache com o servidor de infraestrutura WEM.

- **/wem_cloud_connectors**

  Lista separada por vírgulas de Citrix Cloud™ Connectors no local do recurso que contém a implantação WEM.

- **/wem_server**

  FQDN ou endereço IP do servidor de infraestrutura WEM.

- **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

Depois de instalar um VDA, você pode personalizar várias configurações. No diretório `\x64\XenDesktop Setup` na mídia do produto, execute `XenDesktopVdaSetup.exe`, usando uma ou mais das seguintes opções, que são descritas em Opções de linha de comando para instalar um VDA.

- `/reconfigure` (obrigatório ao personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Solucionar problemas de VDAs

- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição 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.

Opções de linha de comando para instalar um Universal Print Server

A seguinte opção é válida com o comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

SOFTWARE	PASTA	NOME DO ARQUIVO
Recurso de Diagnóstico Citrix	x64 > Virtual Desktop Components	`cdf_x64.msi`
Componente de servidor Universal Print Server	x64 > Universal Print Server	`UpsServer_x64.msi`

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.

Mais informações

Para obter informações sobre como o Citrix relata o resultado das instalações de componentes, consulte Códigos de retorno de instalação do Citrix.

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 ao compartilhamento de rede onde o comando de instalação do VDA está localizado. O comando de instalação é `XenDesktopVdaSetup.exe` no ISO completo do produto, ou `VDAWorkstationSetup.exe` ou `VDAServerSetup.exe` em um instalador autônomo.
- Os detalhes de log são armazenados em cada máquina local. Para registrar os resultados centralmente para revisão e análise, os scripts precisam de acesso de Leitura e Gravação para Todos ao compartilhamento de rede apropriado.

Para verificar os resultados da execução de um script, examine o compartilhamento de log central. Os logs capturados incluem o log do script, o log do instalador e os logs de instalação 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`. Por exemplo, a versão 7 pode ser especificada como 7.0. 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`.

3. Usando os Scripts de Inicialização da Política de Grupo, atribua o script à OU que contém suas máquinas. Esta OU deve conter apenas máquinas nas quais você deseja instalar o VDA. Quando as máquinas nessa OU são reiniciadas, o script é executado em todas elas. Um VDA é instalado em cada máquina que possui um sistema operacional compatível.

Remover VDAs usando o script

1. Obtenha o script de exemplo UninstallVDA.bat de `\Support\AdDeploy\` na mídia de instalação. A Citrix recomenda que você faça um backup do script original antes de personalizá-lo.
2. Edite o script.
   - Especifique a versão do VDA a ser removida: `SET CHECK\_VDA\_VERSION`. Por exemplo, a versão 7 pode ser especificada como 7.0. 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 os Scripts de Inicialização da Política de Grupo, atribua o script à OU que contém suas máquinas. Esta OU deve conter apenas máquinas das quais você deseja remover o VDA. Quando as máquinas na OU são reiniciadas, o script é executado em todas elas. O VDA é removido de cada máquina.

Solução de problemas

- O script gera arquivos de log internos que descrevem o progresso da execução do script. O script copia um log `Kickoff_VDA_Startup_Script` para o compartilhamento de log central em segundos após o início da implantação. Você pode verificar se o processo geral está funcionando. Se este log não for copiado para o compartilhamento de log central conforme o esperado, solucione o problema inspecionando a máquina local. O script coloca dois arquivos de log de depuração na pasta `%temp%` em cada máquina:
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Revise esses logs para garantir que o script esteja:
  - Executando conforme o esperado.
  - Detectando corretamente o sistema operacional de destino.
  - Corretamente configurado para apontar para o `ROOT` do compartilhamento `DEPLOYSHARE` (contém o arquivo chamado `AutoSelect.exe`).
  - Capaz de autenticar-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 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.

Instalar VDAs usando SCCM

> **Nota:**

> A Citrix não se responsabiliza por problemas que surjam causados pela implantação de um Virtual Delivery Agent (VDA) usando ferramentas de distribuição de software, como o Microsoft System Center Configuration Manager (SCCM), adaptadas para corresponder aos

> ambientes de produção do cliente. Para quaisquer problemas relacionados à instalação da Citrix, abra um caso de suporte técnico com os logs de instalação relevantes usando o portal de Suporte da Citrix.

Visão geral

Para implantar com sucesso um Virtual Delivery Agent (VDA) usando o Microsoft System Center Configuration Manager (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 usar o 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.

Reinicializações

O número necessário de reinicializações durante a instalação do VDA depende do ambiente. Por exemplo:

- Uma reinicialização pode ser necessária para atualizações pendentes ou reinicializações de instalações de software anteriores.
- Arquivos 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.

O SCCM Task Sequencer gerencia todas as reinicializações necessárias.

Definir a sequência de tarefas

Após identificar todos os pré-requisitos e reinicializações, use o SCCM Task Sequencer para concluir o seguinte:

- O VDA pode ser instalado 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.

- Ao atualizar um VDA, a máquina na qual ele está instalado deve estar em modo de manutenção, sem sessões.
- Quando uma instalação de VDA é executada pela primeira vez em uma máquina, o instalador de VDA que está sendo usado é copiado para essa máquina.
    - Ao usar um instalador de VDA diferente de `VDAWorkstationCoreSetup_XXXX.exe`, o instalador de VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
    - Ao usar `VDAWorkstationCoreSetup_XXXX.exe`, o instalador de VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`. `
- O local do diretório do instalador de VDA também é armazenado no registro `“HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”`.
- Adicione as opções de linha de comando `/NOREBOOT`, `/NORESUME` e `/QUIET` às suas opções de linha de comando.
    - `/QUIET`: Não mostre a interface do usuário durante a instalação, para que o SCCM tenha controle do processo de instalação.
    - `/NOREBOOT`: Suprima o instalador de VDA de reiniciar automaticamente. O SCCM aciona reinicializações quando necessário.
    - `/NORESUME`: Geralmente, quando uma reinicialização é necessária durante a instalação, o instalador de VDA define uma chave de registro `runonce` (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). Quando a máquina reinicia, o Windows usa a chave para iniciar o instalador de VDA. Isso é um problema para o SCCM, porque o SCCM não pode monitorar a instalação e capturar o código de saída.

Exemplo de sequência de instalação usando SCCM

O exemplo a seguir mostra a sequência de instalação.

1. **TAREFA1 DO SCCM:** Prepare a máquina reiniciando-a.
2. **TAREFA2 DO SCCM:** Inicie a instalação do VDA.

    a. Adicione as opções `/quiet`, `/noreboot` e `/noresume` às suas opções de linha de comando.

b. Execute o instalador de VDA de sua escolha (imagem local ou um dos instaladores mínimos).

c. O SCCM deve capturar o código de retorno.

- Se o código de retorno for 0 ou 8, a instalação está completa e é necessário reiniciar.
- Se o código de retorno for 3, reinicie a máquina e, em seguida, passe o controle para a TAREFA3 do SCCM.

3. **TAREFA3 do SCCM:** Continue a instalação do VDA.

a. Se a TAREFA2 do SCCM não retornar 0 ou 8, a instalação deve ser continuada após a conclusão da reinicialização.

b. A TAREFA3 do SCCM se repete até que o instalador do VDA retorne 0 ou 8 (indicando uma instalação bem-sucedida), ou 3 (indicando que a TAREFA3 do SCCM deve ser repetida). Trate qualquer outro código de retorno como um erro, e a TAREFA3 do SCCM 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 local onde foi copiado (conforme descrito em Definir a sequência de tarefas), sem parâmetros de linha de comando. (O instalador do VDA usa os parâmetros que salvou durante a primeira execução do instalador.)

d. Observe o código de retorno do instalador do VDA.

- 0 ou 8: Sucesso, instalação concluída, reinicialização necessária.
- 3: A instalação não está completa. Reinicie a máquina e repita a TAREFA3 do SCCM até que 0 ou 8 seja retornado. Trate qualquer outro código de retorno como um erro, e a TAREFA3 do SCCM deve relatar um erro e terminar.

Para obter mais informações sobre códigos de retorno, consulte Códigos de retorno de instalação do Citrix.

Exemplos de comandos de instalação do VDA

As opções de instalação disponíveis variam, dependendo do instalador usado. 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 comando a seguir usa o instalador VDA principal de sessão única (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- O comando a seguir usa o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /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
  ```

Criar um site

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 SDK do Citrix Virtual Apps and Desktops 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 **Configuração** no painel de navegação do Studio, depois a guia **Suporte ao Produto** e siga as orientações. 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 que você saiba o que esperar.

Etapa 1. Abra o Studio e inicie o assistente de criação de site

Abra o Studio se ele ainda não estiver aberto. Você será automaticamente guiado para a ação que inicia o assistente de criação de site. Selecione essa ação.

Etapa 2. Tipo e nome do site

Na página **Introdução**, escolha um tipo de site:

- **Site de entrega de aplicativos e desktops**. Ao criar um site de entrega de aplicativos e desktops, você pode optar por criar um site de implantação completa (recomendado) ou um site vazio. Um site vazio é configurado apenas parcialmente e geralmente é criado por administradores avançados.
- **Site de Acesso Remoto a PC**. Um site de Acesso Remoto a PC permite que usuários designados acessem remotamente seus PCs de escritório por meio de uma conexão segura.

Se você criar uma implantação de entrega de aplicativos e desktops agora, poderá adicionar uma implantação de Acesso Remoto a PC mais tarde. Inversamente, se você criar uma implantação de Acesso Remoto a PC agora, poderá adicionar uma implantação completa mais tarde.

Digite um nome para o site. Depois que o site é criado, seu nome aparece na parte superior do painel de navegação do Studio: **Citrix Studio** (*nome-do-site*).

Etapa 3. Bancos de dados

A página **Bancos de Dados** contém seleções para configurar os bancos de dados do site, de monitoramento e de registro de configuração. Para obter detalhes sobre as opções e requisitos de configuração do banco de dados, consulte Bancos de Dados.

> **Observação:**
>
> Se um SQL Server Always On Listener estiver configurado para criptografia TLS, você poderá ser solicitado a inserir credenciais com permissões de criação de banco de dados. As tentativas de criar o banco de dados ainda falharão mesmo se você inserir credenciais de administrador válidas. Verifique se o certificado do SQL Server inclui o nome DNS do listener nos 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), uma reinicialização ocorrerá após a instalação desse software. Essa reinicialização não ocorrerá se você optar por não instalar o software SQL Server Express para usar como banco de dados do site.

Se você não estiver usando o SQL Server Express padrão, certifique-se de que o software SQL Server esteja instalado nas máquinas antes de criar um site. Requisitos do sistema lista as versões suportadas.

Se você quiser adicionar mais Delivery Controllers ao site e já tiver instalado o software Controller em outros servidores, poderá adicionar esses Controllers a partir desta página. Se você também planeja gerar scripts que configuram os bancos de dados, adicione os Controllers antes de gerar os scripts.

Etapa 4. Licenciamento

> **Observação:**

> 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 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 como os quais este produto pode ser configurado, com base nas licenças atualmente instaladas.

- Se você deseja 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 Citrix Manage Licenses Tool) para usar com este produto, mas ainda não instalou a licença:
  - Clique em **Procurar arquivo de licença**.
  - No explorador de arquivos, localize e selecione a licença que você baixou. Os produtos associados agora aparecem na página **Licenciamento** do assistente de criação do site. Selecione a entrada que deseja usar.
- Se o produto desejado não for exibido, ou se você não tiver licenças alocadas e baixadas, você pode alocar, baixar e instalar uma licença. Para fazer isso, o 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 da 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. Gerenciamento de energia (somente Acesso Remoto a PC)

Consulte Etapa 8. Acesso Remoto a PC.

Etapa 6. Conexão do host, rede e armazenamento

Se você estiver usando VMs em um hipervisor ou outro serviço para entregar aplicativos e desktops, poderá, opcionalmente, criar a primeira conexão com esse host. Você também pode especificar recursos de armazenamento e rede para essa conexão. Após criar o site, você pode modificar 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 Studio para gerenciar desktops em PCs blade dedicados), selecione o tipo de conexão **Nenhum**.
- Se você estiver configurando um site de Acesso Remoto a PC e planeja usar o recurso Wake on LAN, selecione o tipo **Microsoft System Center Configuration Manager**.

Além do tipo de conexão, especifique se você usará ferramentas Citrix (como Machine Creation Services™) ou outras ferramentas para criar VMs.

- Para obter informações especificadas nas páginas **Armazenamento** e **Rede**, consulte Armazenamento do host, Gerenciamento de armazenamento e Seleção de armazenamento.
- Se você tem uma Licença de Direitos Híbridos e adicionou conexões de host de nuvem pública (por exemplo, AWS), essas conexões são listadas aqui. Reinicie o Citrix Studio para visualizar essas conexões de host de nuvem pública.

Etapa 7. Recursos Adicionais

Na página **Recursos Adicionais**, você pode selecionar recursos para personalizar seu site. Ao selecionar a caixa de seleção de um item que requer informações, uma caixa de configuração é exibida.

- **Publicação App-V:** Selecione este recurso se você usa aplicativos de pacotes Microsoft App-V em servidores App-V. Forneça a URL do servidor de gerenciamento App-V e a URL e o número da porta do servidor de publicação App-V.

  Se você usa aplicativos de pacotes App-V apenas em locais de compartilhamento de rede, não precisa selecionar este recurso.

  Você também pode habilitar/desabilitar e configurar este recurso mais tarde no Studio. Para obter mais informações, consulte App-V.

Etapa 8. Acesso Remoto ao PC

Para obter informações sobre implantações de Acesso Remoto ao PC, consulte Acesso Remoto ao 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 ao PC Wake on LAN.

Ao criar um site de Acesso Remoto ao PC:

- Se você estiver usando o recurso Wake on LAN, especifique o endereço, as credenciais e as informações de conexão do Microsoft System Center Configuration Manager na página **Gerenciamento de Energia**.
- Especifique usuários ou grupos de usuários na página **Usuários**. Não há nenhuma ação padrão que adicione automaticamente todos os usuários. Além disso, especifique as informações das contas de máquina (domínio e OU) na página **Contas de Máquina**.

  Para adicionar informações de usuário, clique em **Adicionar Usuários**. Selecione usuários e grupos de usuários e, em seguida, clique em **Adicionar usuários**.

  Para adicionar informações de contas de máquina, clique em **Adicionar contas de máquina**. Selecione as contas de máquina e, em seguida, clique em **Adicionar contas de máquina**. Clique em **Adicionar UOs**. Selecione o domínio e as Unidades Organizacionais e indique se deseja incluir itens em subpastas. Clique em **Adicionar UOs**.

Um catálogo de máquinas chamado `Remote PC User Machine Accounts` é criado automaticamente. O catálogo contém todas as contas de máquina que você adicionou no assistente de criação do site. Um grupo de entrega chamado `Remote PC User Desktops` é criado automaticamente. O grupo contém todos os usuários e grupos de usuários que você adicionou.

Etapa 9. Resumo

A página **Resumo** lista as informações que você especificou. Use o botão **Voltar** se quiser alterar algo. Quando terminar, clique em **Criar** e a criação do site será iniciada.

Testar uma configuração de site

Para executar os testes depois de criar o site, selecione **Citrix Studio (Site** *nome-do-site*)** na parte superior do painel de navegação. Em seguida, clique em **Testar site** no painel central. Você pode visualizar um relatório HTML dos resultados do teste do site.

A funcionalidade de teste de site pode falhar para um Controller instalado no Windows Server 2016. A falha ocorre quando um SQL Server Express local é usado para o banco de dados do site e o serviço SQL Server Browser não está iniciado. Para evitar essa falha, conclua as seguintes tarefas.

1. Habilite o serviço SQL Server Browser (se necessário) e, em seguida, inicie-o.
2. Reinicie o serviço SQL Server (SQLEXPRESS).

Os testes de site são executados automaticamente quando você atualiza uma implantação anterior. Para obter detalhes, consulte Testes de site preliminares.

Solução de problemas

Após configurar o site, você pode instalar o Studio e adicioná-lo através do MMC como um snap-in em uma máquina remota. Se você tentar remover esse snap-in posteriormente, o MMC poderá parar de responder. Como solução alternativa, reinicie o MMC.

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.

Se você deseja usar conexões de host de nuvem pública em sua implantação, você precisa da Licença de Direitos Híbridos para concluir sua nova instalação ou atualização para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização pausa ou para. Uma mensagem explicativa aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Efeito da Licença de Direitos Híbridos nas conexões de host

Existem três cenários em que a conexão de host com os hosts de nuvem pública é afetada com base no direito à Licença de Direitos Híbridos:

- Para criar uma conexão de host com os hosts de 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 hosts de 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 catálogos e atualizar imagens
  - Executar ações de energia
- Quando as conexões de host não autorizadas mudam para autorizadas, as conexões de hospedagem existentes são reativadas.

Introdução

Coleções de máquinas físicas ou virtuais são gerenciadas como uma única entidade chamada catálogo de máquinas. As máquinas em um catálogo têm o mesmo tipo de sistema operacional: SO multi-sessão ou SO de sessão única. Um catálogo contendo máquinas com SO multi-sessão pode conter máquinas Windows ou Linux, mas não ambas.

O Citrix Studio o orienta a criar o primeiro catálogo de máquinas depois de criar o site. Depois de criar o primeiro catálogo, o Studio o orienta a 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 ferramentas Citrix, como Machine Creation Services™ (MCS) ou Citrix Provisioning (anteriormente Provisioning Services). 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 usar o Citrix Provisioning para criar máquinas, consulte a documentação Citrix Provisioning para obter instruções.
- Se você usar 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 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 snapshot.
- 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 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 Citrix Studio não realiza a verificação de licenças válidas do Microsoft RDS ao criar um catálogo de máquinas que contém máquinas com SO multi-sessão Windows. Para visualizar o status da licença do Microsoft RDS para uma **máquina com SO multi-sessão** Windows, vá para o Citrix Director. Visualize o status da licença do Microsoft RDS no painel **Detalhes da Máquina**. Este painel está localizado na página **Detalhes da Máquina e Detalhes do Usuário**. Para obter mais informações, consulte Integridade da licença do Microsoft RDS.

Registro de VDA

Um VDA deve ser registrado com um Delivery Controller™ ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos 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 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 adicionar 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 máquina. Por exemplo, se uma mensagem indicar que as informações podem não ser obtidas sobre uma máquina, adicione a máquina mesmo assim.

Para obter 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 contém as alterações feitas durante as sessões. É permanente para desktops dedicados. Para desktops agrupados, ele é excluído e um novo é criado após cada 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 do MCS cria um disco estilo cache de gravação para cada VM. Em ambientes de virtualização XenServer, VMware e SCVMM, o MCS coloca o disco de cache de gravação (WBC) no mesmo local de armazenamento que o disco do SO se você configurar a lista de armazenamento de SO disponível da mesma forma que a lista de armazenamento temporário disponível ao criar uma conexão de host.
- O MCS adicionou a capacidade de usar clones completos em oposição ao cenário de disco Delta descrito na seção anterior.

Recursos do hipervisor também podem entrar na equação. Por exemplo:

- Citrix Hypervisor IntelliCache cria um Disco de Leitura no armazenamento local para cada Citrix Hypervisor. Esta opção economiza IOPS em relação à imagem mestre, que pode estar armazenada no local de armazenamento compartilhado.

- Sobrecarga do hypervisor

  Hipervisores diferentes usam arquivos específicos que criam sobrecarga para VMs. Os hipervisores também usam armazenamento para gerenciamento e operações de registro geral. Calcule o espaço para incluir a sobrecarga para:

  - Arquivos de log
  - Arquivos específicos do hipervisor. Por exemplo:
    - O VMware adiciona mais arquivos à pasta **VM storage**. Consulte Melhores Práticas do VMware.
    - Calcule os requisitos totais de tamanho da sua máquina virtual. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de troca e 100 MB para arquivos de log, consumindo um total de 36,1 GB.
  - Snapshots para XenServer; Snapshots para VMware.

- Sobrecarga de processo

  A criação de um catálogo, a adição de uma máquina e a atualização de um catálogo têm implicações de armazenamento únicas. Por exemplo:

  - Criação inicial do catálogo requer que uma cópia do disco base seja copiada para cada local de armazenamento.

    - Também exige que você crie uma VM de Preparação temporariamente.
  - Adicionar uma máquina a um catálogo não requer a cópia do disco base para cada local de armazenamento. A criação do catálogo varia com base nos recursos selecionados.
  - Atualizar o catálogo para criar um disco base extra em cada local de armazenamento. As atualizações do catálogo também experimentam um pico temporário de armazenamento onde cada VM no catálogo tem 2 discos Diff por um certo período de tempo.

Mais considerações:

- **Dimensionamento da RAM:** Afeta o tamanho de certos arquivos e discos do hypervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de snapshot.
- **Thin / Thick provisioning:** O armazenamento NFS é preferido devido aos recursos de provisionamento thin.

Otimização de armazenamento do Machine Creation Services (MCS)

Com o recurso de otimização de armazenamento do Machine Creation Services (MCS), conhecido como MCS I/O:

- O contêiner de cache de gravação é *baseado em arquivo*, a mesma funcionalidade encontrada no Citrix Provisioning. Por exemplo, o nome do arquivo de cache de gravação do Citrix Provisioning é `D:\vdiskdif.vhdx` e o nome do arquivo de cache de gravação do MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico incluindo suporte para um arquivo de despejo de memória do Windows gravado no disco de cache de gravação.
- O MCS I/O mantém a tecnologia *cache na RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação de várias camadas mais otimizada. Essa funcionalidade permite que um administrador equilibre o custo em cada camada, RAM e disco, e o desempenho para atender à expectativa de carga de trabalho desejada.

A atualização do método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. O MCS I/O não suporta mais cache somente RAM. Especifique um tamanho de disco no Citrix Studio durante a criação do catálogo de máquinas.
2. O disco de cache de gravação da VM é criado e formatado automaticamente ao inicializar uma VM pela primeira vez. Assim que a VM estiver ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.

3. O arquivo de paginação é redirecionado para este volume formatado, `MCSWCDisk`. Como resultado, esse tamanho de disco considera a quantidade total de espaço em disco. Ele inclui o delta entre o tamanho do disco e a carga de trabalho gerada mais o tamanho do arquivo de paginação. Isso geralmente está associado ao tamanho da RAM da VM.

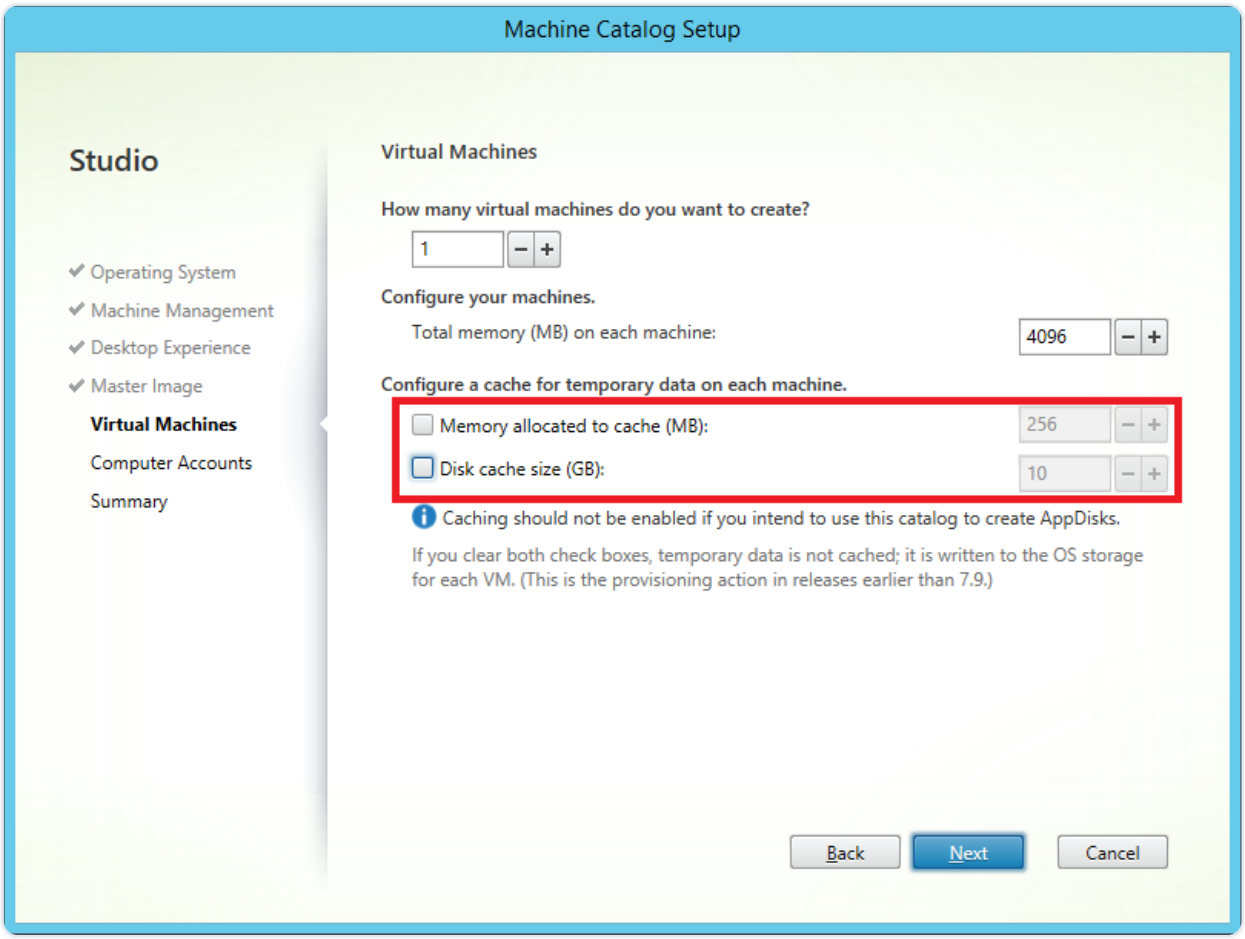
Habilitando atualizações de otimização de armazenamento do MCS

Para habilitar a funcionalidade de otimização de armazenamento MCS I/O, atualize o Delivery Controller e o VDA para a versão mais recente do Citrix Virtual Apps and Desktops.

> **Observação:**
>
> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será necessária. A atualização do VDA e do Delivery Controller manipular a atualização do MCS I/O.

> Ao habilitar a atualização de otimização de armazenamento do MCS, considere o seguinte:

- Ao criar um catálogo de máquinas, o administrador pode configurar o tamanho da RAM e do disco.



- 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 o tamanho da RAM e 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 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 tamanho extra do arquivo de paginação. O tamanho do arquivo de paginação está tipicamente 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.

Usando o PowerShell para criar um catálogo com disco de cache de gravação persistente

Para configurar um catálogo com disco de cache de gravação persistente, use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de gravação persiste para máquinas provisionadas pelo 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 gravação quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Citrix Studio.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de gravação quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Citrix Studio.

Observação:

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 usando o Citrix 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
```

Preparar uma imagem mestre

Para obter informações sobre como criar hosts de conexão, consulte Conexões e recursos.

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

É bom saber:

- Uma imagem mestre também pode ser conhecida como imagem de clone, imagem dourada, VM base ou imagem base. Os fornecedores de host usam termos diferentes.
- Ao usar o Citrix Provisioning, você pode usar uma imagem mestre ou um computador físico como dispositivo de destino mestre. O Citrix Provisioning usa uma terminologia diferente do MCS para se referir a imagens. Consulte a documentação do Citrix Provisioning para obter detalhes.

- 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.
- Considerações sobre a ativação do Microsoft KMS ao usar o MCS: Se sua implantação incluir VDAs 7.x com um host XenServer 6.1 ou 6.2, vSphere ou Microsoft System Center Virtual Machine Manager, você não precisará rearmar manualmente o Microsoft Windows ou o Microsoft Office.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou VMware tools). Se você omitir esta etapa, os aplicativos e desktops podem não funcionar corretamente.
- Um VDA. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais recentes. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros conforme necessário, como software antivírus ou agentes de distribuição eletrônica de software. Configure os serviços com configurações apropriadas para os usuários e o tipo de máquina (como recursos de atualização).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda virtualizar aplicativos. A virtualização reduz custos, eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduzem o tamanho dos discos rígidos da imagem mestre, o que economiza custos de armazenamento.
- Clientes App-V com as configurações recomendadas, se você planeja publicar aplicativos App-V. O cliente App-V está disponível na Microsoft.
- Ao usar o MCS, se você localizar o Microsoft Windows, instale as localidades e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam as localidades e os pacotes de idiomas instalados.

> **Importante:**

> Se você estiver usando o Citrix Provisioning ou 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 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. Ao usar o Citrix Provisioning, crie um arquivo VHD para o disco virtual a partir do seu dispositivo de destino mestre antes de ingressar o dispositivo de destino mestre em um domínio. Consulte a documentação do Citrix Provisioning para obter detalhes.
5. 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.
6. 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 Studio criará um snapshot. Você não pode nomeá-lo.

Criar um catálogo de máquinas usando o Studio

Antes de iniciar o assistente de criação de catálogo, revise esta seção.

Se você estiver usando uma imagem mestre, certifique-se de ter instalado um VDA na imagem antes de criar o catálogo.

No Studio:

- Se você já criou um site, mas ainda não criou um catálogo de máquinas, o Studio o guiará para o local de início correto para criar um catálogo.
- Se você já criou um catálogo e deseja criar outro, selecione **Catálogos de Máquinas** no painel de navegação do **Studio**. Em seguida, selecione **Criar Catálogo de Máquinas** no painel **Ações**.

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 qual ferramenta você usa para implantar máquinas.

Escolha se as máquinas no catálogo são gerenciadas por energia através do Studio.

- As máquinas são gerenciadas por energia através do Studio, por exemplo, VMs ou PCs blade. Esta opção está disponível apenas se você já configurou uma conexão com um host.
- As máquinas não são gerenciadas por energia através do Studio, por exemplo, máquinas físicas.

Se você indicou que as máquinas são gerenciadas por energia através do Studio, escolha qual ferramenta usar para criar VMs.

- **Citrix Machine Creation Services (MCS):** Usa uma imagem mestre para criar e gerenciar máquinas virtuais. O MCS não está disponível para máquinas físicas.
- **Citrix Provisioning:** (Anteriormente Provisioning Services.) Gerencia dispositivos de destino como uma coleção de dispositivos. Um disco virtual do Citrix Provisioning, criado a partir de um dispositivo de destino mestre, entrega desktops e aplicativos.

> **Observação:**
>
> Esta opção não é mais suportada. Para importar um dispositivo de destino do Citrix Provisioning para um catálogo do Citrix Virtual Apps and Desktops, use o **Assistente de Exportação de Dispositivos do Citrix Provisioning**.

- **Outro:** Uma ferramenta que gerencia máquinas já existentes no data center. A Citrix recomenda que você use o Microsoft System Center Configuration Manager ou outro aplicativo de terceiros para garantir que as máquinas no catálogo sejam consistentes.

Tipos de desktop (experiência de desktop)

Esta página aparece somente quando você está criando um catálogo que contém máquinas de SO de sessão única.

A página **Experiência de Desktop** determina o que ocorre cada vez que um usuário faz logon. Selecione uma das opções:

- Os usuários se conectam a um novo desktop (aleatório) cada vez que fazem logon.
- Os usuários se conectam ao mesmo desktop (estático) cada vez que fazem logon.

Se você escolher a segunda opção e estiver usando o MCS para provisionar as máquinas, você pode configurar como as alterações do usuário no desktop são tratadas:

- Salvar as alterações do usuário no desktop no disco local.
- Descartar as alterações do usuário e limpar o desktop virtual quando o usuário fizer logoff. Selecione esta opção se você estiver usando a camada de personalização do usuário.

Imagem mestre

Esta página aparece apenas quando você está usando o MCS para criar VMs.

Na página **Imagem mestre**, selecione a conexão com o host e, em seguida, selecione o snapshot ou a VM criada anteriormente. Se você estiver criando o primeiro catálogo, a única conexão disponível é a que você configurou ao criar o site.

Lembre-se:

- Ao usar o MCS ou o Citrix Provisioning, não execute o Sysprep em imagens mestre.
- Se você especificar uma imagem mestre em vez de um snapshot, o Studio cria um snapshot, mas você não pode nomeá-lo.

Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada. Não altere a seleção mínima padrão do VDA. No entanto, se você precisar usar uma versão anterior do VDA, consulte Versões do VDA e níveis funcionais.

Uma mensagem de erro aparece se você selecionar um snapshot ou VM que não seja compatível com a tecnologia de gerenciamento de máquinas selecionada anteriormente no assistente.

Coleção de Dispositivos

Esta página aparece somente ao usar o Citrix Provisioning para criar VMs.

A página **Coleção de Dispositivos** exibe as coleções de dispositivos e os dispositivos que ainda não foram adicionados aos catálogos.

Selecione as coleções de dispositivos a serem usadas.

Máquinas

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

O título desta página depende do que você selecionou na página **Gerenciamento de Máquinas**: **Máquinas**, **Máquinas Virtuais** ou **VMs e usuários**.

Ao usar o MCS:

- Especifique quantas máquinas virtuais devem ser criadas.
- 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 o Citrix Provisioning:

A página **Dispositivos** lista as máquinas na coleção de dispositivos que você selecionou na página anterior do assistente. Você não pode adicionar ou remover máquinas nesta página.

Ao usar outras ferramentas:

Adicione (ou importe uma lista de) nomes de contas de máquina do Active Directory. Você pode alterar o nome da conta do Active Directory para uma VM depois de adicioná-la/importá-la. Se você especificou máquinas estáticas na página **Experiência da Área de Trabalho**, você pode, opcionalmente, especificar o nome de usuário do Active Directory para cada VM que você 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 o Citrix Provisioning ou outras ferramentas (mas não o MCS):

Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada, ou de uma coleção de dispositivos do Citrix Provisioning) ajudam a identificar máquinas que podem não ser elegíveis para adicionar ao catálogo, ou que podem não conseguir se registrar em um Delivery Controller. Para obter detalhes, consulte Versões de VDA e níveis funcionais.

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) da imagem mestre. (Padrão = clones finos)

- Use clones de cópia rápida para um uso de armazenamento mais eficiente e criação de máquina mais rápida.
- Use clones de cópia completa para melhor recuperação de dados e suporte à migração, com IOPS potencialmente reduzidos após a criação das máquinas.

Versões de VDA e níveis funcionais

O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto exige 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 impacta o nível funcional. Nesses casos, o nível funcional pode indicar uma versão do VDA anterior aos componentes instalados ou atualizados. Por exemplo, embora a versão 7.17 contenha um VDA 7.17, o nível funcional padrão ("7.9 ou posterior") permanece o mais atual. Portanto, após instalar ou atualizar os componentes 7.9–7.16 para 7.17, você não precisa alterar o nível funcional padrão. O artigo Novidades de cada versão indica qualquer alteração no nível funcional padrão.

O nível funcional selecionado afeta a lista de máquinas acima dele. Na lista, uma dica de ferramenta ao lado de cada entrada indica se o VDA da máquina é compatível com o catálogo nesse nível funcional.

Mensagens são exibidas na página se o VDA em cada máquina não atender ou exceder o nível funcional mínimo selecionado. Você pode continuar com o assistente. É provável que essas máquinas não consigam se registrar em um Controller mais tarde. Alternativamente, você pode:

- Remover as máquinas que contêm VDAs mais antigos da lista, atualizar seus VDAs e, em seguida, adicioná-las de volta ao catálogo.
- Escolher um nível funcional inferior que 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 errado. Exemplos incluem tentar adicionar um servidor a um catálogo de SO de sessão única, ou adicionar uma máquina de SO de sessão única originalmente criada para alocação aleatória a um catálogo de máquinas estáticas.

Importante:

Na versão 1811, um nível funcional extra foi adicionado: **1811 (ou mais recente)**. Esse nível é destinado ao uso com futuros recursos do Citrix Virtual Apps and Desktops. A seleção **7.9 (ou mais recente)** permanece como padrão. Esse padrão é válido para todas as implantações agora.

Se você selecionar **1811 (ou mais recente)**, quaisquer versões anteriores de VDA nesse catálogo não conseguirão se registrar em um Controller. No entanto, se o catálogo contiver apenas VDAs na versão 1811 ou versões posteriores suportadas, todos eles serão elegíveis para registro. Isso inclui catálogos que contêm VDAs configurados para versões posteriores do Citrix Virtual Apps and Desktops, incluindo a versão 1903 e outras versões 19XX anteriores à 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.

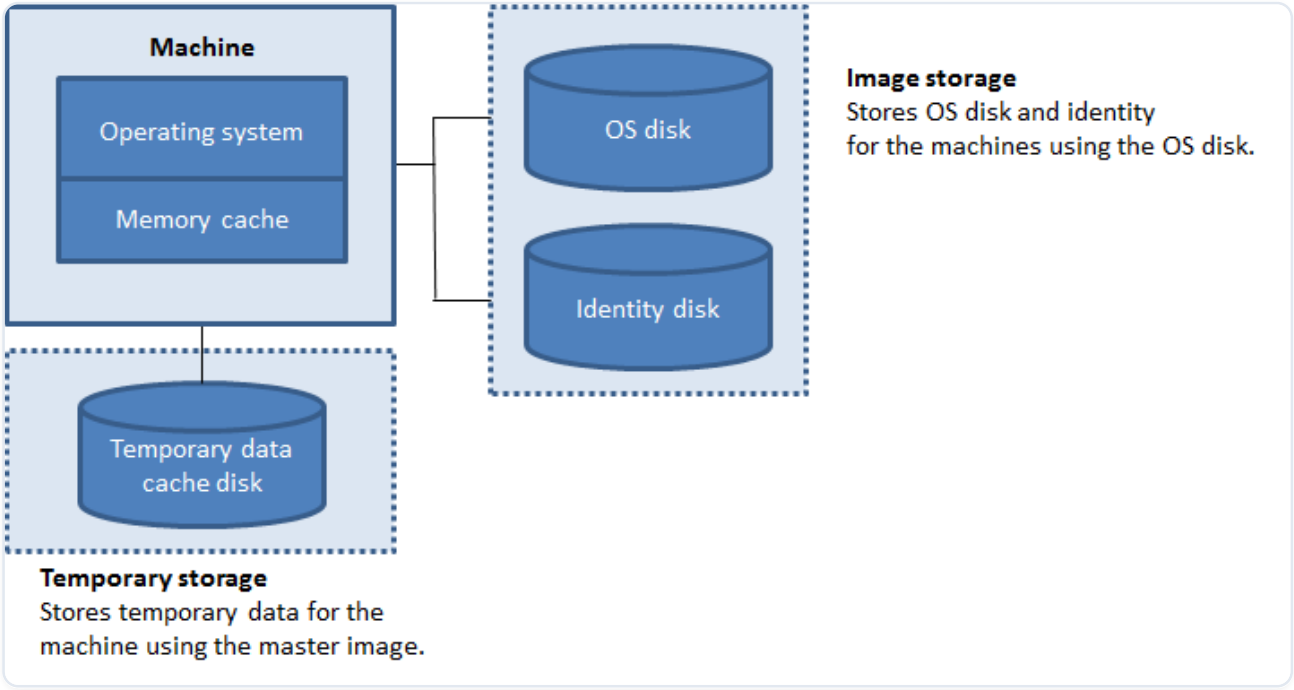
Importante:

Este recurso requer um driver de E/S MCS 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 diferir. Geralmente, os valores padrão são

> suficientes para a maioria dos casos. No entanto, leve em consideração o espaço necessário para:

- Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
- Dados de perfil de usuário.
- Dados do ShareFile que são sincronizados com as sessões dos usuários.
- Dados que podem ser criados ou copiados por um usuário de 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 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 não selecionar a caixa de seleção Memória alocada para cache, os dados temporários serão gravados diretamente no disco de cache, usando uma quantidade mínima de cache de memória.
- 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 inicialmente gravados 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.

Nota:

- 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 em 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 para 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 somente ao criar catálogos de Acesso Remoto para 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.

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.

Contas de computador

Esta página aparece somente ao usar o MCS para criar VMs.

Cada máquina no catálogo deve ter uma conta de computador do Active Directory correspondente. Na página **Contas de Computador**, indique se deseja criar contas ou usar contas existentes, e o local para essas contas.

- Se você criar contas, deverá ter permissão para criar contas de computador na OU onde as máquinas residem.

  Especifique o esquema de nomenclatura da conta para a máquina, usando sinais de hash para indicar onde aparecem números ou letras sequenciais. 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.
- Se você usar contas existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo .csv contendo nomes de contas. O conteúdo do arquivo importado deve usar o formato:

```
[ADComputerAccount]

ADcomputeraccountname.domain

...
```

Certifique-se de que há contas suficientes para todas as máquinas que você está adicionando. O Studio gerencia essas contas, então permita que o Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

Para catálogos contendo máquinas físicas ou máquinas existentes, selecione ou importe contas existentes. Atribua cada máquina a uma conta de computador do Active Directory e a uma conta de usuário.

Para máquinas criadas com o Citrix Provisioning, as contas de computador para dispositivos de destino são gerenciadas de forma diferente; consulte a documentação do Citrix Provisioning.

Resumo, nome e descrição

Na página **Resumo**, revise as configurações especificadas. Insira um nome e uma descrição para o catálogo. Essas informações aparecem no Studio.

Quando terminar, clique em **Concluir** para iniciar a criação do catálogo.

Solucionar problemas

> **Importante:**

> Após criar o catálogo de máquinas usando o Citrix 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 Studio excluir essas tarefas após a criação do catálogo de máquinas, independentemente de o catálogo ser criado com sucesso.

> A Citrix recomenda coletar logs para ajudar a equipe de Suporte a fornecer soluções. Ao usar o Citrix Provisioning, use o seguinte procedimento para gerar arquivos de log:

1. Na imagem mestre, crie a seguinte chave de registro com o valor 1 (como um valor DWORD (32 bits)): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Desligue a imagem mestre e crie um instantâneo.
3. No Delivery Controller, execute o seguinte comando PowerShell: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Crie um catálogo com base nesse instantâneo.
5. Quando a VM de preparação for criada no hipervisor, faça login e extraia os seguintes arquivos da raiz de `C:\`: Image-prep.log e PvsVmAgentLog.txt.
6. Desligue a máquina, momento em que ela relata a falha.
7. Execute o seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Próximos passos

Se este for o primeiro catálogo criado, o Studio o guiará para criar um grupo de entrega.

Gerenciar catálogos de máquinas

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 do 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 atualizar com eficiência um grande número de máquinas de usuário.
- Para máquinas criadas usando o Citrix Provisioning™, as atualizações para as máquinas são propagadas através do disco virtual. Consulte a documentação do Citrix Provisioning para obter detalhes.
- 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 Studio. Execute essa 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 preexistentes continuam a usar a instância original. O processo de atualização de uma imagem é feito da mesma forma que para qualquer outro tipo de catálogo. Considere o seguinte:

- Com catálogos de disco persistentes, as máquinas pré-existentes não são atualizadas para a nova imagem, mas quaisquer novas máquinas adicionadas ao catálogo usam a nova imagem.
- Para catálogos de disco não persistentes, a imagem da máquina é atualizada na próxima vez que a máquina for redefinida.
- Com catálogos de máquinas persistentes, a atualização da imagem também atualiza as instâncias do catálogo que a utilizam.
- Para catálogos que não persistem, se você quiser imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

Adicionar máquinas a um catálogo

Antes de começar:

- Certifique-se de que o host de virtualização tenha processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- Certifique-se de ter contas de computador do Active Directory não utilizadas suficientes. Se você estiver usando contas existentes, o número de máquinas que você pode adicionar é limitado pelo número de contas disponíveis.
- Se você usar o Studio para criar contas de computador do Active Directory para as máquinas adicionais, você deve ter a permissão de administrador de domínio apropriada.

Para adicionar máquinas a um catálogo:

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar máquinas** no painel **Ações**.
3. Selecione o número de máquinas virtuais a serem adicionadas.
4. Se não houver contas do Active Directory existentes suficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas. Especifique um esquema de nomenclatura de conta, usando sinais de cerquilha para indicar onde números ou letras sequenciais aparecem. Não use uma barra (/) em um nome de 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.

5. 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 haja contas suficientes para todas as máquinas que você está adicionando. O Studio gerencia essas contas. Permita que o Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

As máquinas são criadas como um processo em segundo plano e podem levar muito tempo ao criar muitas máquinas. A criação da máquina continua mesmo se você fechar o Studio.

Excluir máquinas de um catálogo

Depois de excluir uma máquina de um catálogo de máquinas, os usuários não poderão mais acessá-la, portanto, antes de excluir uma máquina, certifique-se de que:

- Os dados do usuário são copiados ou não são mais necessários.
- Todos os usuários estão desconectados. Ativar o modo de manutenção impede que novas conexões sejam feitas a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Exibir Máquinas** no painel **Ações**.
3. Selecione uma ou mais máquinas e, em seguida, selecione **Excluir** no painel **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 serão retidas, desabilitadas ou excluídas.

Alterar a descrição de um catálogo ou alterar as configurações de Acesso Remoto a PC

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Editar Catálogo de Máquinas** no painel **Ações**.

3. Para o catálogo de Acesso Remoto para PC, use a página **Gerenciamento de Energia** para alterar as configurações de gerenciamento de energia e selecionar uma conexão de gerenciamento de energia. Na página **Unidades Organizacionais**, adicione ou remova UOs do Active Directory.
4. Na página **Descrição**, altere a descrição do catálogo.

Renomear um catálogo

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Renomear Catálogo de Máquinas** no painel **Ações**.
3. 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. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Mover** no painel **Ações**.
3. 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 estão desconectados e nenhuma sessão desconectada está em execução.
- O modo de manutenção está ativado para todas as máquinas no catálogo para que novas conexões não possam ser feitas.
- Todas as máquinas no catálogo estão desligadas.
- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.

2. Selecione um catálogo e, em seguida, selecione **Excluir Catálogo de Máquinas** no painel **Ações**.
3. 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 múltiplas 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. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Gerenciar contas AD** no painel **Ações**.
3. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas das contas: redefina todas elas ou insira uma senha que se aplique a todas as contas.

   Você pode redefinir senhas se não souber as senhas atuais 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.

Para catálogos que usam Citrix Provisioning (anteriormente Provisioning Services), você deve publicar um novo disco virtual para aplicar as alterações ao catálogo. Para obter detalhes, consulte a documentação do Citrix Provisioning.

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 no 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 Studio. Embora o 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 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 Citrix Hypervisor™.

Atualizar o catálogo

Para preparar e implantar a atualização em todas as máquinas de um catálogo:

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione um catálogo e, em seguida, selecione **Atualizar Máquinas** no painel **Ações**.
3. Na página **Imagem Mestre**, selecione o host e a imagem que você deseja implantar.
4. 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.

5. Verifique as informações na página **Resumo** e clique em **Concluir**. Cada máquina é reiniciada automaticamente após ser atualizada.

Ao atualizar um catálogo usando o PowerShell SDK diretamente, em vez do Studio, especifique um modelo de hipervisor (modelos de VM). Use isso como uma alternativa a uma imagem ou um instantâneo de uma imagem.

Estratégia de implantação:

A atualização da imagem 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 multissessão com máquinas filhas, as reinicializações não ocorrem automaticamente. Para aplicar a imagem mestre atualizada, reinicie as máquinas usando o Studio, PowerShell ou Workspace. Reiniciar 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.
>
> Se você optar por atualizar a imagem imediatamente, configure um tempo de distribuição e notificações.

- **Tempo de distribuição:** Escolha atualizar todas as máquinas ao mesmo tempo ou especifique a duração total para começar a atualizar todas as máquinas no catálogo. Um algoritmo interno determina quando cada máquina é atualizada e reiniciada durante esse intervalo.
- **Notificação:** No menu suspenso de notificação à esquerda, escolha se deseja exibir uma mensagem de notificação nas máquinas antes que uma atualização comece. Por padrão,

nenhuma mensagem é exibida. Escolha exibir uma mensagem 15 minutos antes do início da atualização. Ou, escolha repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não é repetida. A menos que você escolha atualizar todas as máquinas ao mesmo tempo, a mensagem de notificação é exibida em cada máquina no momento apropriado antes do início da atualização.

Reverter uma atualização

Depois de implantar uma imagem mestre atualizada/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. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione o catálogo e, em seguida, selecione **Reverter atualização da máquina** no painel **Ações**.
3. Especifique quando aplicar a imagem mestre anterior às máquinas, conforme descrito na seção anterior para a operação de implantação.

A reversão é aplicada apenas às máquinas que precisam ser revertidas. Máquinas que não foram atualizadas com a imagem mestre nova/atualizada não recebem mensagens de notificação e não são forçadas a fazer logoff.

Atualizar um catálogo ou reverter uma atualização

Atualize o 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 novos.

Antes de atualizar um catálogo:

- Se você estiver usando o Citrix Provisioning, atualize a versão do VDA. O console de provisionamento não retém a versão do VDA. O Citrix Provisioning se comunica diretamente com o Assistente de Configuração do Citrix Virtual Apps and Desktops™ para definir a versão do VDA no catálogo criado.
- Inicie as máquinas atualizadas para que elas se registrem no Controller. Esse processo permite que o Studio determine que as máquinas no catálogo precisam ser atualizadas.

Para atualizar um catálogo:

1. Selecione **Catálogos de Máquinas** no painel de navegação do **Studio**.
2. Selecione o catálogo. A guia **Detalhes** no painel inferior exibe as informações da versão.
3. Selecione **Atualizar Catálogo**. Se o Studio detectar que o catálogo precisa ser atualizado, ele exibirá uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser atualizadas, uma mensagem explicará o motivo. A Citrix recomenda que você resolva os problemas da máquina antes de atualizar o catálogo para garantir que todas as máquinas funcionem corretamente.

Após a conclusão da atualização do catálogo, você pode reverter as máquinas para suas versões VDA anteriores selecionando o catálogo e, em seguida, selecionando **Desfazer** no painel **Ações**.

Alterar a configuração de rede para um esquema de provisionamento existente

Você pode alterar a configuração de rede para um esquema de provisionamento existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede.

> **Observação:**

> Este recurso é compatível com Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versões posteriores.

> Para alterar a configuração de rede de um esquema de provisionamento existente, faça o seguinte:

1. Na janela do PowerShell, execute o comando `asnp citrix*` para carregar os módulos do PowerShell.
2. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para acessar o caminho de rede que você deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

```
$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.

Solução de problemas

- Para máquinas com status "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.

Criar grupos de entrega

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. Mais tarde, você pode alterar as configurações iniciais no primeiro grupo de entrega e criar outros grupos de entrega. Existem também recursos e configurações que você pode configurar apenas ao editar um grupo de entrega, e não ao criá-lo.

Para Acesso Remoto a PC, quando você cria 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 Studio o guiará para o local de partida correto para criar um. Se você já criou um grupo de entrega e deseja criar outro, selecione **Delivery Groups**. Selecione **Create Delivery Group** no painel Ações.
2. O assistente é iniciado com uma página de **Introdução**, que você pode remover de futuras inicializações deste assistente.
3. 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 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 tipo de SO, mas não de ambos.
- A Citrix recomenda que você instale ou atualize todas as máquinas com a versão mais recente do VDA. Atualize catálogos e grupos de entrega conforme necessário. Ao criar um grupo de entrega, se você selecionar máquinas que possuem 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 outras máquinas tiverem a versão atual, todas as máquinas do grupo poderão usar apenas os recursos que eram suportados no VDA 7.1. Isso significa que alguns recursos que exigem versões posteriores do VDA podem não estar disponíveis nesse grupo de entrega.
- Cada máquina em um catálogo de Acesso Remoto a PC é automaticamente associada a um grupo de entrega. Ao criar um site de Acesso Remoto a PC, um catálogo chamado "Remote PC Access Machines" e um grupo de entrega chamado "Remote PC Access Desktops" 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 RemotePC
  - Verificação relacionada ao AppDisk

Etapa 2. Tipo de entrega

Esta página aparece somente se você escolheu um catálogo contendo máquinas OS 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 SO de várias sessões ou de um catálogo aleatório (agrupado) de SO de sessão única, o tipo de entrega é considerado aplicativos e desktops: você pode entregar aplicativos, desktops ou ambos.

Etapa 3. 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 quando você cria ou edita o seguinte:

- Uma lista de acesso de usuário de um site, que não é configurada através do Studio. Por padrão, a regra da política de direito de aplicativo inclui 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 direito de aplicativo padrão que inclui todos.
- Configure a lista de usuários do grupo de entrega para permitir que todos os usuários da sede usem qualquer um dos aplicativos especificados no grupo de entrega.
- (Se os grupos de aplicativos estiverem configurados) Configure a lista de usuários do grupo de aplicativos para permitir que os membros da unidade de negócios de Administração e Finanças acessem os aplicativos A a L.
- Configure as propriedades do aplicativo A para restringir sua visibilidade apenas à equipe de Contas a Receber em Administração e Finanças.

Usuários autenticados e não autenticados

Existem dois tipos de usuários: autenticados e não autenticados (não autenticados também são chamados de anônimos). Você pode configurar um ou ambos os tipos em um grupo de entrega.

- **Autenticados:** Para acessar aplicativos e desktops, os usuários e membros do grupo que você especificar pelo nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha ao StoreFront ou ao aplicativo Citrix Workspace™. Para grupos de entrega que contêm máquinas de SO de sessão única, você pode importar dados de usuário (uma lista de usuários) posteriormente, editando o grupo de entrega.
- **Não autenticados (anônimos):** Para grupos de entrega que contêm máquinas de SO de várias 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 da 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 os usuários não autenticados estão habilitados, você deve ter uma loja StoreFront não autenticada.

  Contas de usuário não autenticadas são criadas sob demanda quando uma sessão é iniciada e são nomeadas Anon*XYZ*, onde *XYZ* é um valor exclusivo de três dígitos.

  Sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desconectadas automaticamente quando o cliente se desconecta. Reconexão, roaming entre clientes e Workspace Control não são suportados.

A tabela a seguir descreve suas escolhas na página **Usuários**:

HABILITAR ACESSO PARA	ADICIONAR/ATRIBUIR USUÁRIOS E GRUPOS DE USUÁRIOS?	HABILITAR A CAIXA DE SELEÇÃO "CONCEDER ACESSO A USUÁRIOS NÃO AUTENTICADOS"?
Apenas usuários autenticados	Sim	Não
Apenas usuários não autenticados	Não	Sim

HABILITAR ACESSO PARA	ADICIONAR/ATRIBUIR USUÁRIOS E GRUPOS DE USUÁRIOS?	HABILITAR A CAIXA DE SELEÇÃO "CONCEDER ACESSO A USUÁRIOS NÃO AUTENTICADOS"?
Usuários autenticados e não autenticados	Sim	Sim

Etapa 4. Aplicativos

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega do 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.
- Quando você adiciona 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 peça para 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 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 fonte, uma nova página é iniciada com uma lista de aplicativos descobertos; selecione os que deseja adicionar e clique em **OK**.
- **Definido manualmente:** Aplicativos localizados no site ou em outro lugar da sua rede. A seleção desta fonte inicia uma nova página onde você digita o caminho para o executável, o

diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Depois de inserir essas informações, clique em **OK**.

- **Existente:** Aplicativos adicionados anteriormente ao site, talvez em outro grupo de entrega. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Adicione os aplicativos e clique em **OK**.
- **App-V:** Aplicativos em pacotes App-V. Ao selecionar esta fonte, uma nova página é iniciada 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 App-V.

Se uma fonte de aplicativo ou aplicativo não estiver disponível ou for inválida, ele não estará visível ou não poderá ser selecionado. Por exemplo, a fonte **Existente** não está 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 5. 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 "Applications" 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 aplicativo Citrix Workspace.
- Para adicionar uma restrição de tag a um desktop, selecione **Restringir inicializações a máquinas com esta tag** e, em seguida, selecione a tag na lista suspensa. Para obter mais informações, consulte Tags.
- Use os botões de opção para iniciar um desktop ou para atribuir uma máquina ao iniciar o desktop. Os usuários podem ser todos que podem acessar este grupo de entrega, ou usuários e grupos de usuários específicos.

- Se o grupo contiver máquinas atribuídas, especifique o número máximo de desktops por usuário. Este deve ser um valor de um ou mais.
- 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 de usar a caixa de diálogo, clique em **OK**.

Número máximo de instâncias de um desktop em um site (somente PowerShell)

Para configurar o número máximo de instâncias de um desktop no site (somente PowerShell):

- No PowerShell, use o cmdlet BrokerEntitlementPolicyRule apropriado com o parâmetro MaxPerEntitlementInstances. Por exemplo, o cmdlet a seguir modifica a regra `tsvda-desktop` para definir o número máximo de instâncias simultâneas de um desktop permitidas no site para duas. Quando há duas instâncias de desktop em execução, ocorre um erro se um terceiro assinante tentar iniciar um desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- Para obter orientação, use o cmdlet Get-Help. Por exemplo, `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`.

Etapa 6. Resumo

Insira um nome para o grupo de entrega. Você também pode (opcionalmente) inserir uma descrição, que aparece no aplicativo Citrix Workspace e no Studio.

Revise as informações de resumo e clique em **Concluir**.

Gerenciar grupos de entrega

Introdução

Este artigo descreve procedimentos para gerenciar grupos de entrega a partir do console de gerenciamento. Além de alterar as configurações especificadas ao criar o grupo, você pode configurar outras configurações que não estão disponíveis ao criar um grupo de entrega.

As categorias de procedimento incluem: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Impedir que usuários se conectem a máquinas"

é descrito na categoria de máquinas, mas também afeta os usuários. Se você não conseguir encontrar uma tarefa em uma categoria, verifique uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Aplicativos contêm informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer as permissões da função interna de Administrador de Grupo de Entrega. Para obter detalhes, consulte Administração delegada.

Geral

- Alterar o tipo de entrega
- Alterar endereços do StoreFront™
- Atualizar um grupo de entrega
- Gerenciar grupos de entrega do Acesso Remoto para PC

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 de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Alterar endereços do StoreFront

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **StoreFront**, selecione ou adicione URLs do StoreFront. Essas URLs são usadas pelo aplicativo Citrix Workspace™ app, que está 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 **OK** para aplicar as alterações e fechar a janela.

Você também pode especificar endereços de servidor StoreFront selecionando **Configuração > StoreFront** no painel de navegação.

Atualizar um grupo de entrega ou reverter uma atualização

Atualize um grupo de entrega depois de atualizar os Virtual Delivery Agents (VDAs) em suas máquinas e os catálogos de máquinas que contêm as máquinas usadas no grupo de entrega.

Antes de iniciar a atualização do grupo de entrega:

- 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 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 atualizar um grupo de entrega:

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Atualizar Grupo de Entrega** no painel Ações. A ação **Atualizar Grupo de Entrega** aparece somente se VDAs atualizados forem detectados.

A exibição indica quais máquinas, se houver, não podem ser atualizadas e por quê. Você pode então cancelar a atualização, resolver os problemas da máquina e iniciar a atualização novamente.

Após a conclusão da atualização, você pode reverter as máquinas para seus estados anteriores selecionando o grupo de entrega e clicando em **Desfazer** no painel **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 de navegação.
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**.

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 de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 **OK** 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.

CONFIGURAÇÃO	DESCRIÇÃO
Fuso horário	O fuso horário em que as máquinas deste grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site.
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 de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Usuários**:
    - Para adicionar usuários, clique em **Adicionar** e 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 **OK** 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 do usuário de um arquivo .csv depois de criar o grupo de entrega. Você também pode exportar informações do usuário para um arquivo .csv. O arquivo .csv pode conter dados de uma versão anterior do produto.

A primeira linha no arquivo CSV deve conter dois cabeçalhos de coluna, separados por vírgula. Certifique-se de que o primeiro cabeçalho seja `Machine Account` e o segundo cabeçalho seja `User Names`. (Você pode incluir cabeçalhos adicionais, mas eles não são suportados.) As linhas subsequentes no arquivo contêm dados separados por vírgula. As entradas `Machine Account` podem ser SID do computador, FQDN ou pares de nome de domínio e computador.

Para importar ou exportar informações do usuário:

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 **OK** 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 o 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
- Carregar máquinas gerenciadas
- Ligar/desligar 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. Não é possível alterar as atribuições para máquinas de SO de várias sessões ou máquinas provisionadas com Citrix Provisioning.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 **OK** 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 de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Atualizar uma máquina em um grupo de entrega

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Exibir Máquinas** no painel Ações.
3. Selecione uma máquina e clique em **Atualizar Máquinas** no painel Ações.

Para escolher uma imagem diferente, selecione **Imagem mestre** e, em seguida, selecione um instantâneo.

Para aplicar as alterações e notificar os usuários da máquina, selecione **Notificação de lançamento para usuários finais**. Em seguida, especifique:

- Quando atualizar a imagem mestre: agora ou na próxima reinicialização
- O tempo de distribuição da reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados da reinicialização
- A mensagem que os usuários recebem

Adicionar, alterar ou remover uma restrição de tag para um desktop

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais desktops são considerados para lançamento. Revise as considerações e precauções em Tags.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Desktops**, selecione a área de trabalho 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 **OK** para aplicar as alterações e fechar a janela.

Remover uma máquina de um grupo de entrega

Remover uma máquina a exclui de um grupo de entrega. Isso não a exclui do catálogo de máquinas que o grupo de entrega usa. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes de serem removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto você a remove, coloque a máquina em modo de manutenção antes de desligá-la.

As máquinas podem conter dados pessoais, portanto, tenha cuidado antes de alocar a máquina a outro usuário. Considere refazer a imagem da máquina.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Exibir Máquinas** no painel Ações.
3. Certifique-se de que a máquina esteja desligada.
4. Selecione a máquina e clique em **Remover do Grupo de Entrega** no painel 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 o acesso para usuários por meio de expressões de política SmartAccess:** Use expressões de política para filtrar as conexões de usuário feitas por meio do Citrix Gateway.

  a. Selecione **Grupos de Entrega** no painel de navegação.

  b. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.

  c. Na página **Política de Acesso**, selecione **Conexões por meio do NetScaler® Gateway**.

  d. Para escolher um subconjunto dessas conexões, selecione **Conexões que atendem a qualquer um dos seguintes filtros**. Em seguida, defina o site do Citrix Gateway e adicione, edite ou remova as expressões de política SmartAccess para os cenários de acesso de usuário permitidos. Para obter detalhes, consulte a documentação do Citrix Gateway.

  e. 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.

- **Restringir o acesso para usuários por meio 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 o 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 **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo.
3. Para ativar o modo de manutenção para todas as máquinas no grupo de entrega, clique em **Ativar Modo de Manutenção** no painel Ações.

   Para ativar o modo de manutenção para uma máquina, clique em **Exibir Máquinas** no painel Ações. Selecione uma máquina e, em seguida, clique em **Ativar Modo de Manutenção** no painel 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 **Desativar Modo de Manutenção** no painel 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.
- O RDC está definido como **Não permitir conexões a este computador**.
- O RDC não está definido como **Não permitir conexões a este computador**. A configuração **Modo de Logon do Usuário da Configuração do Host Remoto** é **Permitir reconexões, mas impedir novos logons** ou **Permitir reconexões, mas impedir novos logons até que o servidor seja reiniciado**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, o que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, o que afeta as máquinas nesse catálogo.

Desligar e reiniciar máquinas em um grupo de entrega

Este procedimento não é suportado para máquinas de Acesso Remoto a PC.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e, em seguida, clique em **Exibir Máquinas** no painel Ações.
3. Selecione a máquina e, em seguida, clique em uma das seguintes entradas no painel 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 terminem.

A Citrix recomenda que você impeça que usuários de máquinas com 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

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 aos itens que possuem a tag.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você deseja que cada máquina seja reiniciada uma vez por semana e que as máquinas usadas pela equipe de contabilidade sejam reiniciadas diariamente. Para conseguir isso, configure um agendamento para todas as máquinas e outro agendamento apenas para as máquinas da contabilidade.

Um agendamento inclui o dia e a hora em que a reinicialização começa, e a duração.

Você pode ativar ou desativar um agendamento. Desativar um agendamento pode ser útil durante testes, em intervalos especiais ou ao preparar agendamentos antes de precisar deles.

Você não pode usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reiniciar.

> **Nota:**
>
> O Citrix Studio não oferece suporte à configuração de agendamento de reinicialização para sistemas operacionais de desktop.

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 é projetado para evitar reiniciar a mesma máquina com mais frequência do que o pretendido, mas isso não pode ser garantido.

- Se os agendamentos coincidirem precisamente nos horários de início e duração, é mais provável que as máquinas sejam reiniciadas apenas uma vez.
- Quanto mais os agendamentos diferirem nos horários de início e duração, mais provável será que ocorram várias reinicializações.
- O número de máquinas afetadas por um agendamento também afeta a chance de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário para máquinas de contabilidade, dependendo da duração especificada para cada um.

Para uma análise aprofundada dos agendamentos de reinicialização, consulte Detalhes internos do agendamento de reinicialização.

Visualizar agendamentos de reinicialização

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 habilitado.

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 reinício pode especificar apenas uma tag.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione o grupo que contém as máquinas controladas pelo agendamento.
3. Clique em **Exibir Máquinas** e selecione as máquinas às quais você deseja adicionar uma tag.
4. Clique em **Gerenciar Tags** no painel Ações.
5. Se a tag existir, marque a caixa de seleção ao lado do nome da tag. Se a tag não existir, clique em **Criar** e especifique o nome da tag. Depois que a tag for criada, marque a caixa de seleção ao lado do nome da tag recém-criada.
6. Clique em **Salvar** na caixa de diálogo **Gerenciar Tags**.

Criar um agendamento de reinício

> **Nota:**

> Os agendamentos de reinício podem ser aplicados a todas as máquinas multissessão gerenciadas por energia e não gerenciadas por energia.

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Agendamento de Reinicialização**, clique em **Adicionar**.
4. Na página **Add Restart Schedule**:

    - Digite um nome e uma descrição para o agendamento.
    - Se você estiver usando uma restrição de tag, selecione a tag.
    - Em **Frequência de reinício**, selecione a frequência com que o reinício ocorre: diariamente, dias de semana, fins de semana ou um dia específico a cada semana.
    - Usando o relógio de 24 horas, especifique a hora do dia para iniciar o reinício.
    - Para **Duração do reinício**, escolha se todas as máquinas são reiniciadas ao mesmo tempo, ou a duração total para iniciar o reinício de todas as máquinas afetadas. Um algoritmo interno determina quando cada máquina é reiniciada durante esse intervalo.

    > **Nota:**
    >
    > Outra opção de duração de reinício está disponível ao usar o PowerShell. Consulte Reiniciar após o esvaziamento.

    - Em **Enviar notificação aos usuários**, escolha se deseja exibir uma mensagem de notificação nas máquinas afetadas antes do início de um reinício. Por padrão, nenhuma mensagem é exibida.
    - Se você optar por exibir uma mensagem 15 minutos antes do início do reinício, poderá escolher (em Frequência de notificação) repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não é repetida.
    - Insira o título e o texto da notificação. Não há texto padrão.

      Se você quiser que a mensagem inclua o número de minutos antes do reinício, inclua a variável **%m%**. Por exemplo: "Aviso: Seu computador será reiniciado automaticamente em %m% minutos." O valor diminui em cinco minutos em cada mensagem repetida. A menos que você tenha escolhido reiniciar todas as máquinas ao mesmo tempo, a mensagem é

exibida em cada máquina no momento apropriado antes do reinício, calculado pelo algoritmo interno.

- Para ativar o agendamento, marque a caixa de seleção. Para desativar o agendamento, desmarque a caixa de seleção.

5. 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.

Reiniciar após drenagem

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`).

Quando você habilita 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 desconectadas.

Este recurso é compatível com grupos de entrega que contêm máquinas de sessão única ou multi-sessão. As máquinas devem ter o gerenciamento de energia ativado.

Em um ambiente local, este recurso é compatível apenas ao usar o PowerShell. O recurso não está disponível no Studio.

Editar, remover, habilitar ou desabilitar um agendamento de reinicialização

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel 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 reinicialização.
    - Para habilitar ou desabilitar um agendamento, clique em **Editar**. Marque ou desmarque a caixa de seleção **Habilitar agendamento de reinicialização**.
    - Para remover um agendamento, clique em **Remover**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma tag aplicada às máquinas nas máquinas afetadas.

Reinicializações agendadas atrasadas devido a interrupção do banco de dados

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

> Se ocorrer uma interrupção do banco de dados do site antes do início de uma reinicialização agendada para máquinas (VDAs) em um grupo de entrega, as reinicializações começarão quando a interrupção terminar. Isso pode ter resultados não intencionais.

Por exemplo, digamos que você agendou as reinicializações de um grupo de entrega para ocorrerem fora do horário de produção (começando às 03:00). Uma interrupção do banco de dados do site ocorre uma hora antes do início de uma reinicialização agendada (02:00). A interrupção dura seis horas (até as 08:00). O agendamento de reinicialização começa quando a conexão entre o Delivery Controller e o banco de dados do site é restaurada. As reinicializações dos VDAs agora começam cinco horas após o agendamento original, 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 esse valor ao configurar um agendamento de reinicialização no Studio.

Reinicializações agendadas para máquinas em modo de manutenção

> **Nota:**

> Este recurso está disponível apenas no PowerShell.

> Para indicar se um agendamento de reinicialização afeta máquinas que estão em modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria um agendamento que reinicia 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.

Gerenciar carga de máquinas em grupos de entrega

Você pode gerenciar a carga apenas de máquinas de SO multi-sessão.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as condições atuais do ambiente. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** Uma máquina de SO multi-sessão é considerada para balanceamento de carga somente quando o modo de manutenção está desativado.
- **Índice de carga do servidor:** Determina a probabilidade de um servidor que entrega máquinas de SO multi-sessão receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações para métricas de desempenho, como uso de CPU, disco e memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga.

  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 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 detalhes, consulte CTX202150.

- **Configuração da política de tolerância de logon simultâneo**: O número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões do XenApp 6.x.)

  Quando todos os servidores estão no nível ou acima da configuração de tolerância de logon simultâneo, a próxima solicitação de logon é atribuída ao servidor com o menor número de logons pendentes. Se mais de um servidor atender a esses critérios, o servidor com o menor índice de carga será selecionado.

Máquinas com gerenciamento de energia em um grupo de entrega

Você pode gerenciar a energia apenas de máquinas virtuais de SO de sessão única, não de máquinas físicas (incluindo máquinas de Acesso Remoto a PC). Máquinas de SO de sessão única com recursos de GPU não podem ser suspensas, portanto, as operações de desligamento falham. Para máquinas de SO de várias sessões, você pode criar um agendamento de reinicialização.

Em grupos de entrega que contêm máquinas em pool, as máquinas virtuais de SO de sessão única podem estar em um dos seguintes estados:

- Alocadas aleatoriamente e em uso
- Não alocadas e desconectadas

Em grupos de entrega que contêm máquinas estáticas, as máquinas virtuais de SO de sessão única podem ser:

- Alocadas permanentemente e em uso
- Alocadas permanentemente e desconectadas (mas prontas)
- Não 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 são 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 especificado. Por exemplo, as máquinas suspendem 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 de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Gerenciamento de Energia**, selecione **Dias úteis** em **Gerenciar energia das máquinas**. Por padrão, os dias úteis são de segunda a sexta-feira.
4. Para grupos de entrega aleatórios, em **Máquinas a serem ligadas**, clique em **Editar** e especifique o tamanho do pool durante os dias úteis. Em seguida, selecione o número de máquinas a serem ligadas.

5. Em **Horas de pico**, defina as horas de pico e fora de pico para cada dia.
6. Defina os temporizadores de estado de energia para horas de pico e fora de pico durante os dias úteis: Em **Durante as horas de pico > Quando desconectado**, especifique o atraso (em minutos) antes de suspender qualquer máquina desconectada no grupo de entrega e, 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 **OK** 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 se aplica apenas a máquinas VDI com sessões desconectadas. Não se aplica a máquinas VDI com sessões encerradas.
>
> Em versões anteriores, uma máquina VDI em transição para um período de tempo onde uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Esse cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) 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 ao fazer a transição do pico para fora do pico. A partir do Citrix Virtual Apps and Desktops 7 1909, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina VDI na transição de período. Como resultado, a máquina é desligada 10 minutos após a transição para fora do pico.

Se você quiser reverter para o comportamento anterior (ou seja, não realizar nenhuma ação em máquinas que fazem a transição 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`, o equivalente a *true*, que habilita o comportamento anterior. Por padrão, o valor é `0`, ou *false*, 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 faz a transição para um período de tempo diferente.
- Ter uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e faz a transição para um período onde uma ação de energia é atribuída.

Alterar a porcentagem de VDAs em estado ligado para catálogos

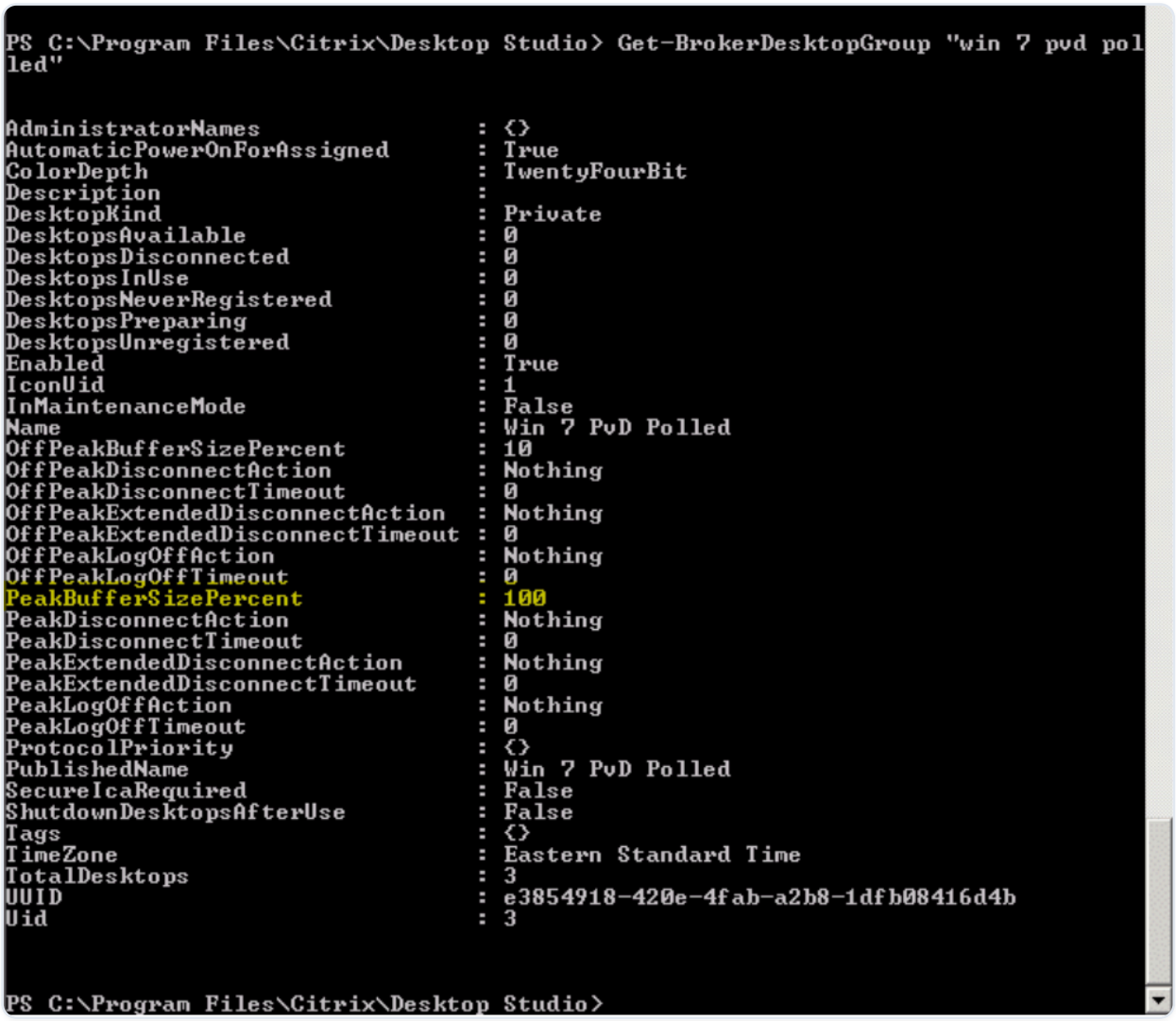
1. Ajuste os horários de pico para o grupo de entrega na seção **Gerenciamento de energia** do grupo de entrega.
2. Anote o nome do Grupo de Área de Trabalho.
3. Com privilégios de administrador, inicie o PowerShell e execute os seguintes comandos. Substitua "Desktop Group Name" pelo nome do seu grupo de área de trabalho que tem uma porcentagem alterada de VDAs em execução.

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   Um valor de 100 significa que 100% dos VDAs estão no estado pronto.
4. Verifique a solução executando:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



Pode levar até uma hora para que as alterações entrem em vigor.

Para desligar os VDAs depois que o usuário fizer logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

Para reiniciar VDAs durante o horário de pico, para que estejam prontos para os usuários depois que eles fizerem logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

Sessões

- Fazer logoff ou desconectar uma sessão, ou enviar uma mensagem aos usuários
- Configurar o pré-lançamento e a permanência da sessão
- Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção

Fazer logoff ou desconectar uma sessão

1. No painel de navegação do Studio, selecione **Delivery Groups**.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** no painel **Actions**.
3. No painel central, selecione a máquina, selecione **View Sessions** no painel **Actions** e, em seguida, selecione uma sessão.
    - Como alternativa, no painel central, selecione a guia **Session** e, em seguida, selecione uma sessão.
4. Para fazer logoff de uma sessão, selecione **Log off** no painel **Actions**. A sessão é fechada e o usuário é desconectado. A máquina fica disponível para outros usuários, a menos que seja alocada para um usuário específico.
5. Para desconectar uma sessão, selecione **Disconnect** no painel **Actions**. Os aplicativos continuam a ser executados na sessão e a máquina permanece alocada para esse usuário. O usuário pode se reconectar à mesma máquina.

Você pode configurar temporizadores de estado de energia para máquinas de SO de sessão única para manipular automaticamente sessões não utilizadas. Para obter detalhes, consulte Máquinas com gerenciamento de energia.

Enviar uma mensagem para um grupo de entrega

1. No painel de navegação do Studio, selecione **Delivery Groups**.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** no painel **Actions**.
3. No painel central, selecione uma máquina para a qual você deseja enviar uma mensagem.
4. No painel **Actions**, selecione **View Sessions**.
5. No painel central, selecione todas as sessões e, em seguida, selecione **Send Message** no painel **Actions**.
6. Digite sua mensagem e clique em **OK**. Você pode especificar o nível de severidade, se necessário. As opções incluem **Crítico**, **Pergunta**, **Aviso** e **Informação**.

Alternativamente, você pode enviar uma mensagem usando o Citrix Director. Para obter mais informações, consulte Enviar mensagens para usuários.

Configurar o pré-lançamento e a permanência da sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas de SO multi-sessão.

Os recursos de pré-lançamento de sessão e de permanência de sessão ajudam usuários específicos 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 Citrix Workspace app para Windows e também exigem configuração extra do Citrix Workspace app. Para obter instruções, procure por pré-lançamento de sessão na documentação do produto para sua versão do Citrix Workspace app 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 concorrente, mas apenas quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. Sessões pré-lançadas e persistentes não utilizadas se desconectam após 15 minutos por padrão. Este valor pode ser configurado no PowerShell (cmdlet `New/Set-BrokerSessionPreLaunch`).
- Um planejamento e 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 licenças em uso e recursos alocados.
- Você também pode configurar o pré-lançamento de sessão para um horário agendado no Citrix Workspace app.

Por quanto tempo as sessões pré-lançadas e persistentes não utilizadas permanecem ativas

Existem várias maneiras de especificar por quanto tempo uma sessão não utilizada permanece ativa se o usuário não iniciar um aplicativo: um tempo limite configurado e limites de carga do servidor. Você pode configurar todos eles. O evento que ocorre primeiro faz com que a sessão não utilizada seja encerrada.

- **Tempo limite:** Um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-lançada ou persistente não utilizada permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-lançadas terminam antes de fornecerem ao usuário o benefício de um acesso mais rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário de entrada podem ser negadas porque o servidor não tem recursos suficientes.

  Você pode habilitar esse tempo limite apenas no SDK (cmdlet `New/Set-BrokerSessionPreLaunch`), não no console de gerenciamento. Se você desabilitar o tempo limite, ele não aparecerá na exibição do console para esse grupo de entrega ou nas páginas **Editar Grupo de Entrega**.
- **Limites:** O encerramento automático de sessões pré-lançadas e persistentes com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, assumindo que os recursos do servidor estejam disponíveis. As sessões pré-lançadas e persistentes não utilizadas não causam conexões negadas porque são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

  Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-lançamento ou persistência por mais tempo são encerradas. As sessões são encerradas uma a uma em intervalos de um minuto até que a carga caia abaixo do limite. Enquanto o limite é excedido, nenhuma nova sessão de pré-lançamento é iniciada.

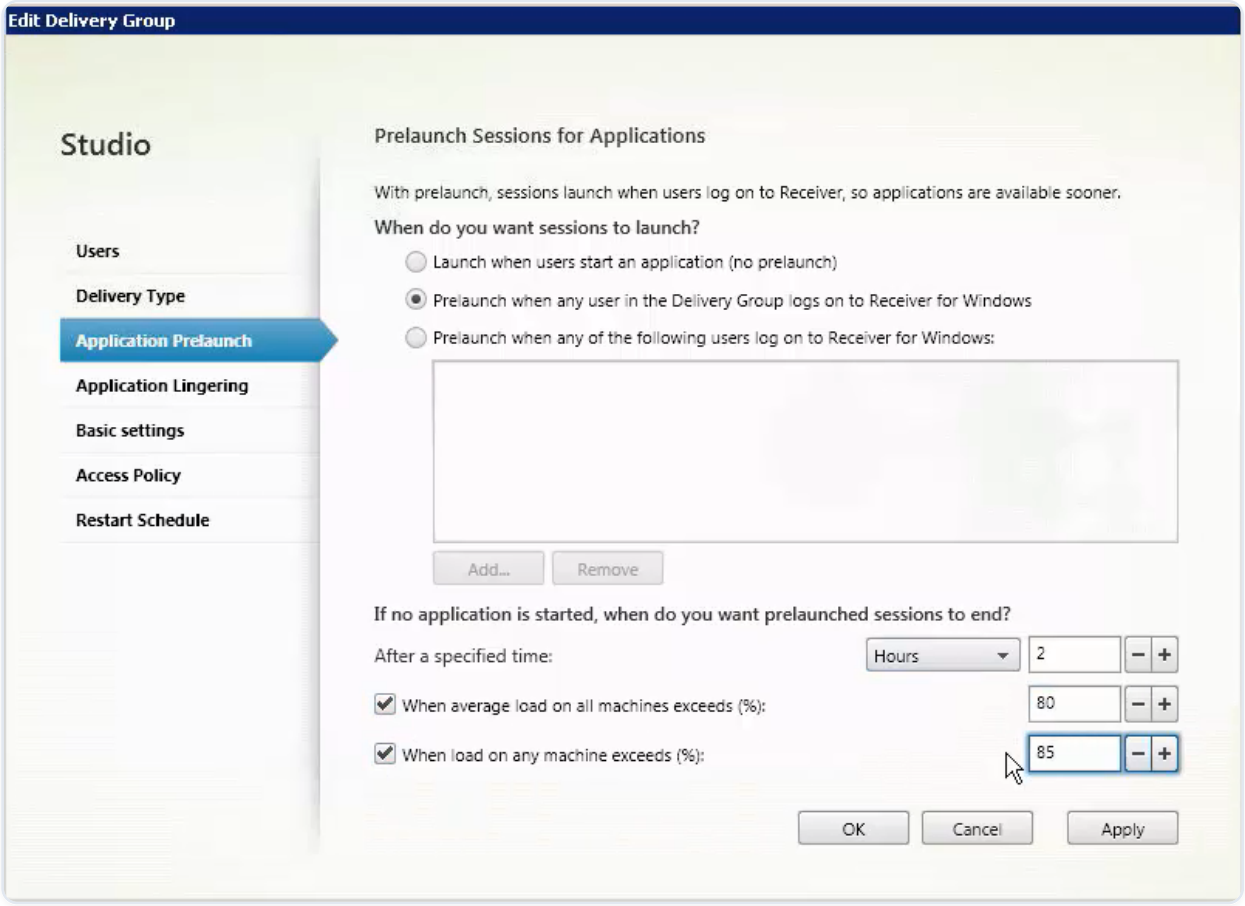
Servidores com VDAs que não se registraram em um Controller e servidores em modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-lançamento e persistentes sejam encerradas automaticamente para liberar capacidade.

Para habilitar o pré-lançamento de sessão

1. Selecione **Grupos de Entrega** no painel de navegação.

2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Pré-lançamento de Aplicativos**, ative o pré-lançamento de sessão escolhendo quando as sessões são iniciadas:

    - Quando um usuário inicia um aplicativo. Esta é a configuração padrão. O pré-lançamento de sessão está desativado.
    - Quando qualquer usuário no grupo de entrega faz logon no Citrix Workspace app para Windows.
    - Quando qualquer pessoa em uma lista de usuários e grupos de usuários faz logon no Citrix Workspace app para Windows. Certifique-se de especificar também usuários ou grupos de usuários se você escolher esta opção.



4. Uma sessão pré-lançada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-lançada não for usada), as seguintes configurações afetam por quanto tempo essa sessão permanece ativa.

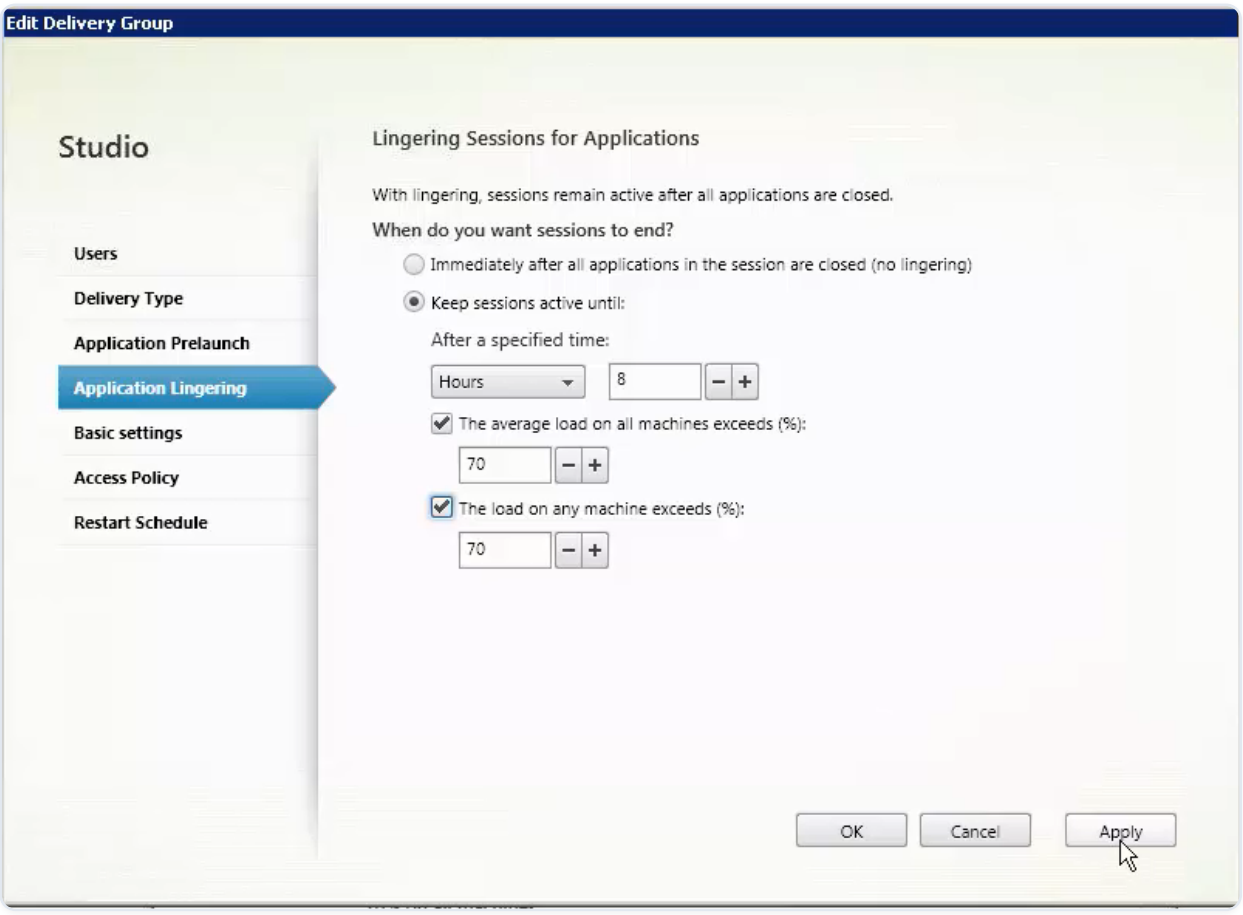
    - Quando um intervalo de tempo especificado decorre. Você pode alterar o intervalo de tempo (1–99 dias, 1–2376 horas ou 1–142.560 minutos).
    - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada (1–99%).

- Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada (1–99%).

Recapitulação: Uma sessão pré-lançada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado decorre ou um limite de carga especificado é excedido.

Para habilitar a permanência da sessão

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** no painel Ações.
3. Na página **Permanência do Aplicativo**, ative a permanência da sessão selecionando **Manter sessões ativas até**.



4. Várias configurações afetam por quanto tempo uma sessão persistente permanece ativa se o usuário não iniciar outro aplicativo.

- Quando um intervalo de tempo especificado expira. Você pode alterar o intervalo de tempo: 1–99 dias, 1–2376 horas ou 1–142.560 minutos.
- Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada: 1–99%.

- Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada: 1–99%.

Recapitulação: Uma sessão persistente permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado expira ou um limite de carga especificado é excedido.

Controlar a reconexão de sessão quando desconectado da máquina em modo de manutenção

> **NOTA:**
>
> Este recurso está disponível apenas no PowerShell.
>
> Você pode controlar se as sessões que são desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes da versão 2106, a reconexão não era permitida para sessões de desktop agrupadas de sessão única que haviam sido desconectadas de máquinas 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
- Multissessão: Habilitado

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 **Solução de problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

  Para mensagens sobre o nível funcional, consulte Versões de VDA e níveis funcionais.

  Para obter informações sobre a solução de problemas de registro de VDA, consulte CTX136668.

- Na exibição de um grupo de entrega, a **versão do VDA instalada** no painel de detalhes pode ser diferente da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas com status de **Estado de Energia Desconhecido**, consulte CTX131267 para obter orientação.

Criar grupos de aplicativos

Introdução

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. 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.

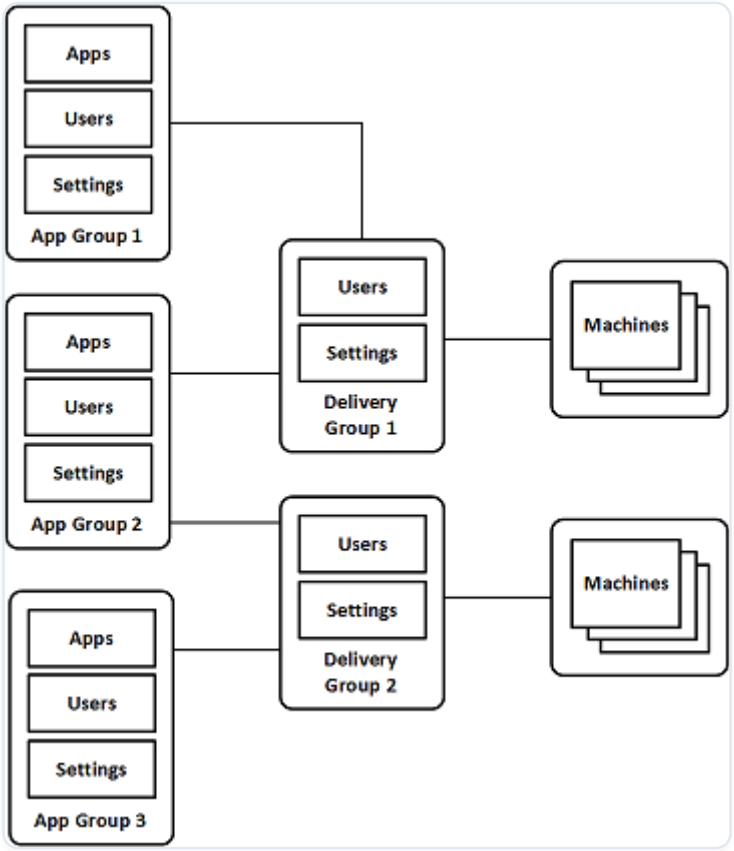
O uso de grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega:

- 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 de cada vez.
- 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 em 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.

Exemplos de configurações

Exemplo 1:

O gráfico a seguir mostra uma implantação do Citrix Virtual Apps and Desktops™ que inclui grupos de aplicativos:



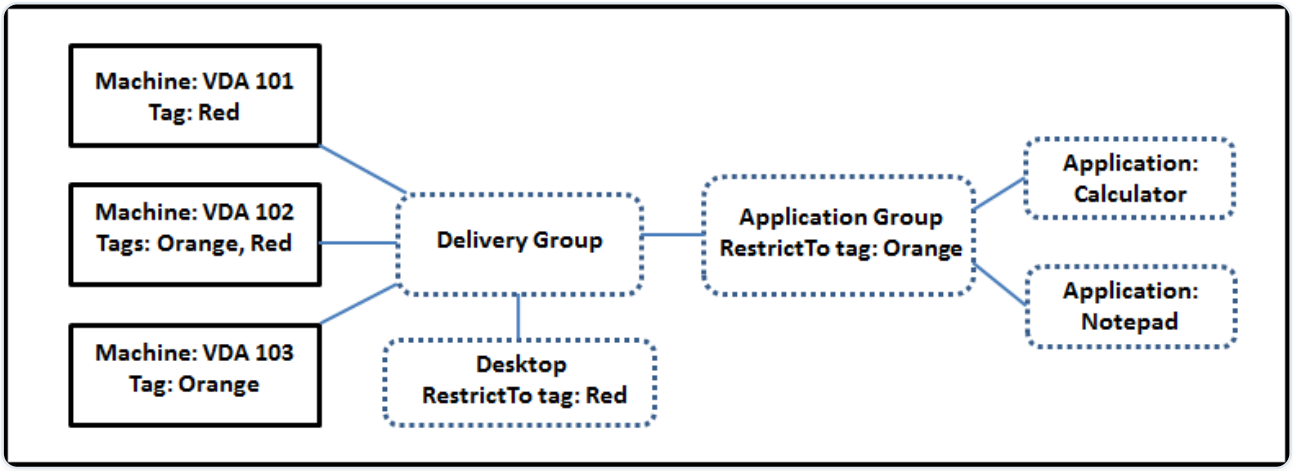
Nesta configuração, os aplicativos são adicionados aos grupos de aplicativos, não aos grupos de entrega. Os grupos de entrega especificam quais máquinas são usadas. (Embora não mostrado, as máquinas estão em catálogos de máquinas.)

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 grupos de entrega, mas não a ambos. Caso contrário, a complexidade adicional de ter aplicativos em dois tipos de grupo pode dificultar o gerenciamento.

Por padrão, um grupo de aplicativos é habilitado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado. Consulte Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. Este processo requer:

1. Atualizar VDAs nas máquinas usadas no grupo de entrega.
2. Atualizar os catálogos de máquinas que contêm essas máquinas.
3. Atualizar o grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ser no mínimo da versão 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo se refere a "associar" um aplicativo a mais de um grupo de aplicativos. Ele diferencia essa ação de adicionar instâncias desse aplicativo de uma fonte disponível. Da mesma forma, os grupos de entrega são associados a grupos de aplicativos, em vez de serem adições ou componentes uns dos outros.

Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão de aplicativo está habilitado, todos os aplicativos são iniciados na mesma sessão de aplicativo. Isso economiza os custos associados ao lançamento de mais sessões de aplicativo e permite o uso de recursos de aplicativo que envolvem a área de transferência, como operações de copiar e colar. No entanto, em algumas situações, você pode desativar o compartilhamento de sessão.

Ao usar grupos de aplicativos, você pode configurar o compartilhamento de sessão de aplicativo das três maneiras a seguir, que estendem o comportamento padrão de compartilhamento de sessão disponível ao usar apenas grupos de entrega:

- Compartilhamento de sessão habilitado entre grupos de aplicativos.
- Compartilhamento de sessão habilitado apenas entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desabilitado.

Compartilhamento de sessão entre grupos de aplicativos

Você pode habilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos, ou pode desabilitá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo em que habilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  O grupo de aplicativos 1 contém aplicativos do Microsoft Office, como Word e Excel. O grupo de aplicativos 2 contém outros aplicativos, como Bloco de Notas e Calculadora, e ambos os grupos de aplicativos estão anexados ao mesmo grupo de entrega. Um usuário que tem acesso a ambos os grupos de aplicativos inicia uma sessão de aplicativo 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 na qual a sessão está sendo executada — então uma nova sessão em uma máquina adequada é criada em vez de usar o compartilhamento de sessão.
- **Um exemplo em que desabilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

Uma configuração com um conjunto de aplicativos que não interoperam bem com outros aplicativos instalados nas mesmas máquinas. Como duas versões diferentes da mesma suíte de software ou duas versões diferentes do mesmo navegador da web. Você prefere não permitir que um usuário inicie ambas as versões na mesma sessão.

Crie um grupo de aplicativos para cada versão da suíte de software e adicione os aplicativos de cada versão da suíte de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desabilitado para cada um desses grupos de aplicativos, um usuário especificado nesses grupos poderá executar aplicativos da mesma versão na mesma sessão. O usuário ainda pode executar outros aplicativos ao mesmo tempo, mas não na mesma sessão. Ao iniciar um dos aplicativos de versão diferente, ou qualquer aplicativo que não esteja contido em um grupo de aplicativos, esse aplicativo é iniciado em uma nova sessão.

Este recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de sandboxing de segurança. Não é infalível e não pode impedir que os usuários iniciem aplicativos em suas sessões por outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver na capacidade máxima, novas sessões não serão iniciadas nela. Novos aplicativos são iniciados em sessões existentes na máquina conforme necessário, usando o compartilhamento de sessão.

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 aplicativos entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo de quando desabilitar o compartilhamento de sessão dentro de grupos de aplicativos é útil:**

Você deseja que seus usuários acessem várias sessões simultâneas em tela cheia de um aplicativo em monitores separados.

Você cria um grupo de aplicativos e adiciona os aplicativos a ele.

Por padrão, o compartilhamento de sessão de aplicativo é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Criar um grupo de aplicativos

Para criar um grupo de aplicativos:

1. Selecione **Aplicativos** no painel de navegação do Studio e, em seguida, selecione **Criar Grupo de Aplicativos** no painel Ações.
2. O assistente é iniciado com uma página de **Introdução**, que você pode remover de futuros lançamentos deste assistente.
3. O assistente o guiará pelas páginas descritas na seção a seguir. Ao terminar cada página, clique em **Avançar** até chegar à página 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. Os grupos de entrega compatíveis contêm máquinas de SO de sessão única ou multi-sessão aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Grupos de Entrega Incompatíveis** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como conter máquinas atribuídas estaticamente.

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.

- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando o assistente de criação de grupo de aplicativos é confirmado.

Embora você possa criar um grupo de aplicativos que não tenha grupos de entrega associados (talvez para organizar aplicativos ou para servir como armazenamento para aplicativos não usados 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 **Iniciar** 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, somente os usuários especificados no grupo de entrega e no grupo de aplicativos poderão 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.

A habilitação ou desabilitação do uso de aplicativos por usuários não autenticados está disponível apenas em grupos de entrega, não em grupos de aplicativos.

Para obter informações sobre onde as listas de usuários são especificadas em uma implantação, consulte Onde as listas de usuários são especificadas.

Etapa 3. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e um com o mesmo nome existir nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você concordar com o nome exclusivo sugerido, o

aplicativo será adicionado com esse novo nome. Caso contrário, você deve renomeá-lo antes que possa ser adicionado. Para obter detalhes, consulte Gerenciar pastas de aplicativos.

- Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Consulte Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Nome do aplicativo (para usuário)** no Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.
- Quando você adiciona um aplicativo a mais de um grupo de aplicativos, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo foi adicionado.

Clique em **Adicionar** no menu suspenso para exibir as fontes do aplicativo.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta fonte não pode ser selecionada se você selecionou qualquer um dos seguintes:

  - Grupos de aplicativos que não têm grupos de entrega associados.
  - Grupos de aplicativos com grupos de entrega associados que não contêm máquinas.
  - Um grupo de entrega que não contém máquinas.

- **Definido manualmente:** Aplicativos localizados no site ou em outro lugar na sua rede. Ao selecionar esta fonte, uma nova página é iniciada onde você digita o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Depois de inserir essas informações, clique em **OK**.
- **Existente**: Aplicativos adicionados anteriormente ao site. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e 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 iniciada onde você seleciona **Servidor App-V** ou **Biblioteca de Aplicativos**. Na exibição resultante, marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**. Para obter mais informações, consulte 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. As fontes que são incompatíveis não são listadas de forma alguma (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

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 de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Habilitar ou desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Para obter mais informações, consulte Compartilhamento de sessão com grupos de aplicativos.

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Desabilitar compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é habilitado por padrão ao criar um grupo de aplicativos. Se você desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanecerá habilitado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão de aplicativo desabilitado entre os aplicativos que eles contêm. Em algumas circunstâncias, essa opção é desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não-seamless em janelas de aplicativo de tamanho completo em monitores separados.

Ao desabilitar o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão de aplicativo. Se uma sessão desconectada adequada estiver disponível e estiver executando o mesmo aplicativo, ela será reconectada. Por exemplo, 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. 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 que estão associados a grupos de aplicativos, mas não estão associados a grupos de entrega. Todos os aplicativos associados diretamente a um grupo de entrega compartilham sessões por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, certifique-se de que os grupos não tenham configurações conflitantes. Por exemplo, um grupo com a opção definida como `True`, e a opção de outro grupo definida como `False` resulta em comportamento imprevisível.

Renomear um grupo de aplicativos

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Renomear Grupo de Aplicativos** no painel 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 de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover uma restrição de tag em um grupo de aplicativos

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais máquinas são consideradas para o lançamento de aplicativos. Revise as considerações e precauções em Tags.

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel Ações.
3. Selecione a página **Grupos de Entrega**.
4. Para adicionar uma restrição de tag, selecione **Restringir lançamentos a máquinas com a tag** e, em seguida, selecione a tag na lista suspensa.
5. Para alterar ou remover uma restrição de tag, selecione uma tag diferente ou remova a restrição de tag completamente desmarcando **Restringir lançamentos a máquinas com esta tag**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Adicionar ou remover usuários em um grupo de aplicativos

Para obter informações detalhadas sobre usuários, consulte Criar grupos de aplicativos.

1. Selecione **Aplicativos** no painel de navegação do Studio.

2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (você não pode editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** no painel 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 **OK** para aplicar as alterações e fechar a janela.

Excluir um grupo de aplicativos

Um aplicativo deve estar associado a pelo menos um grupo de entrega ou grupo de aplicativos. Se a exclusão de um grupo de aplicativos resultar em um ou mais aplicativos que não pertencem mais a um grupo, você será avisado de que a exclusão desse grupo também 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 de navegação do Studio.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Excluir Grupo** no painel Ações.
3. Confirme a exclusão quando solicitado.

Acesso Remoto a 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 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 de múltiplos usuários.

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 com Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:

- Use a opção "/physicalmachine" juntamente com a opção "/remotepc" como parte da instalação do VDA por linha de comando
- Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada não tenha sido usada `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - Nome: ForceEnableRemotePC
  - Tipo: DWORD
  - Dados: 1

Considerações de implantação

Ao planejar a implantação do Acesso Remoto a PC, tome algumas decisões gerais.

- Você pode adicionar o Acesso Remoto a PC a uma implantação existente do Citrix Virtual Apps and Desktops. 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.

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 vários usuários podem acessar remotamente em diferentes turnos.
    - PCs Windows agrupados. Este caso de uso se aplica a PCs físicos que vários usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas de SO de sessão única
    - Estático - PCs Linux dedicados
    - Aleatório - PCs Linux agrupados

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.

- Ao escolher as UOs nas quais as contas de máquina residem, selecione UOs de nível inferior para maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de Banco/Oficiais/Caixas, selecione **Caixas** para maior granularidade. Caso contrário, você pode selecionar **Oficiais** ou **Banco** com base no requisito.
- Mover ou excluir UOs depois de serem atribuídas a um catálogo de máquinas de Acesso Remoto a PC afeta as associações de VDA e causa problemas com atribuições futuras. Portanto, certifique-se de planejar adequadamente para que as atualizações de atribuição de UO para catálogos de máquinas sejam consideradas no plano de alteração do Active Directory.
- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas devido à estrutura da UO, você não precisa selecionar nenhuma UO. Você pode usar o PowerShell para adicionar máquinas ao catálogo posteriormente. As atribuições automáticas de usuário continuam funcionando se a atribuição de desktop estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo de máquinas junto 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 ao PC**.

   b. Na página **Gerenciamento de Energia**, escolha habilitar ou desabilitar o gerenciamento de energia para o catálogo de máquinas padrão de Acesso Remoto ao PC. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.

   c. Preencha as informações nas páginas **Usuários** e **Contas de Máquina**.

A conclusão dessas etapas cria um catálogo de máquinas chamado **Máquinas de Acesso Remoto ao PC** e um Grupo de Entrega chamado **Desktops de Acesso Remoto ao PC**.

3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a. Crie um catálogo de máquinas do tipo **Acesso Remoto ao PC** (página Sistema Operacional do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Certifique-se de atribuir a OU correta para que os PCs de destino fiquem disponíveis para uso com o Acesso Remoto ao PC.

   b. Crie um Grupo de Entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um Grupo de Entrega, consulte Criar Grupos de Entrega. Certifique-se de atribuir o Grupo de Entrega a um grupo do Active Directory que contenha os usuários que precisam de acesso aos seus PCs.

4. Implante o VDA nos PCs do escritório.

   - Recomendamos usar o instalador VDA principal do SO de sessão única (VDAWorkstationCoreSetup.exe).
   - Você também pode usar o instalador VDA completo de sessão única (VDAWorkstationSetup.exe) com a opção `/remotepc`, que alcança o mesmo resultado que usar o instalador VDA principal.
   - Considere habilitar a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto através do Citrix Director. Para fazer isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para poder ver as informações de duração de logon no Director, você deve usar o instalador VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Inclua este componente usando a opção `/includeadditional`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para obter informações sobre como implantar o VDA usando o SCCM, consulte Instalar VDAs usando o SCCM.
   - Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

   Depois de concluir com sucesso as etapas 2 a 4, os usuários são automaticamente atribuídos às suas próprias máquinas quando fazem login localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente que eles usam para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace

está disponível em `https://www.citrix.com/downloads/` ou nas lojas de aplicativos para dispositivos móveis suportados.

Recursos gerenciados através do registro

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

Desabilitar atribuições automáticas de múltiplos usuários

Em cada Delivery Controller™, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dados: 0

Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina de Acesso Remoto a PC entre em estado de suspensão, adicione esta configuração de registro no VDA e, em seguida, reinicie a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra em modo de suspensão após o tempo limite de inatividade pré-configurado. Depois que a máquina acorda, ela se registra novamente com o Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Valor: 1

Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é automaticamente desconectada quando um usuário local inicia uma sessão nessa máquina (pressionando CTRL+ALT+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e, em seguida, reinicie a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Valor: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é reconhecida dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Valor:
  - 1 - O usuário remoto sempre tem preferência se ele ou ela não responder à interface de mensagens no período de tempo limite especificado. Este comportamento é o padrão se esta configuração não for definida.
  - 2 - O usuário local tem preferência.

O tempo limite para aplicar o modo Acesso Remoto ao PC é de 30 segundos por padrão. Você pode configurar esse tempo limite, mas não o defina para menos de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dados: número de segundos para o tempo limite em valores decimais

Quando um usuário deseja obter acesso forçado ao console: O usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local sobre uma sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon nesse PC enquanto ele estiver em uso por um usuário remoto, o usuário remoto receberá um prompt. O prompt pergunta se deve permitir ou negar a conexão do usuário local. Permitir a conexão desconecta a sessão do usuário remoto.

Registro de gerenciamento de sessão

O Acesso Remoto ao PC agora possui recursos de registro que registram quando alguém tenta acessar um PC com uma sessão ICA® ativa. Isso permite que você monitore seu ambiente em busca de atividades indesejadas ou inesperadas e seja capaz de auditar esses eventos se precisar investigar quaisquer incidentes.

Os eventos são registrados usando o Visualizador de Eventos do Windows e estão em **Aplicativos e Serviços > Citrix > HostCore > Serviço ICA > Admin**.

Existem três eventos distintos que são registrados ao usar o Acesso Remoto a PCs.

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
- Origem: Serviço ICA

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
- Origem: Serviço ICA

ID do Evento 46

Este ID de evento aparece quando a sessão remota foi desconectada e quando o valor do registro SasNotification não existe ou o valor do registro SasNotification é 0.

- Mensagem:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

ID do Evento 47

Este ID de evento aparece quando o usuário remoto concorda em desconectar a sessão e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode é 2 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
The remote session for &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 Ctrl+Alt+Del pressionado duas vezes

Este evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

Detalhes do evento

- Nome do log: Aplicativo e Serviços
- ID do Evento: 49
- Origem: Serviço ICA

ID do Evento 49

Este ID de evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

- Mensagem:

```
The remote session for &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 em que o PC reside, quando instruído pelo controlador de entrega. Isso permite que o recurso funcione sem depender 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 herdado baseado em SCCM. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN – Integrado ao SCCM.

Limitação

O Acesso Remoto ao PC com o recurso Wake on LAN não suporta o ligamento automático durante os horários de pico.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes de compatibilidade, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows

Configurar Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops local, a configuração do Wake on LAN integrado é suportada apenas usando o PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas do Acesso Remoto ao PC se você ainda não tiver um.
2. Crie a conexão de host do Wake on LAN se você ainda não tiver uma.

> **Observação:**
>
> Para usar o recurso Wake on LAN, se você tiver uma conexão de host do tipo "Microsoft Configuration Manager Wake on LAN", crie uma nova conexão de host.

3. Recupere o identificador exclusivo da conexão de host do Wake on LAN.
4. Associe a conexão de host do Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host do Wake on LAN:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `
```

```
                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

Quando a conexão de host estiver pronta, execute os seguintes comandos para recuperar o identificador exclusivo da conexão de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Depois de recuperar o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo de máquinas do Remote PC Access:

```
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 Studio. No entanto, a edição de suas propriedades no Studio não é suportada se estiver usando o Citrix Virtual Apps and Desktops local.
- Pacotes mágicos são enviados de uma das duas maneiras:

    a. Quando um usuário tenta iniciar uma sessão em seu PC e o VDA está não registrado

    b. Quando um administrador envia manualmente um comando de ligar do Studio ou PowerShell

- Como o controlador de entrega não tem conhecimento do estado de energia de um PC, o Studio exibe **Não Suportado** sob o estado de energia. O controlador de entrega 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 o Remote PC Access que está disponível apenas com o Citrix Virtual Apps and Desktops local.

Requisitos do sistema

A seguir estão os requisitos de sistema para usar o recurso Wake on LAN integrado ao SCCM:

- Citrix Virtual Apps and Desktops 1912 ou posterior
- PCs físicos:
  - VDA versão 1912 ou posterior
  - Windows 10. Para obter detalhes de suporte, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou posterior

Configurar Wake on LAN integrado ao SCCM

Conclua os seguintes pré-requisitos:

1. Configure o SCCM 2012 R2, 2016 ou 2019 na organização. Em seguida, implante o cliente SCCM em todas as máquinas de Acesso Remoto a 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, ative 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 por 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 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 ao PC:

- Se você estiver criando um novo catálogo de Acesso Remoto ao PC, na página **Sistema Operacional** do assistente de criação de catálogo, selecione **Acesso Remoto ao 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 ao PC existente:

  a. Vá para o nó **Catálogos de Máquinas** no Studio, selecione o catálogo de máquinas e, em seguida, selecione **Editar Catálogo de Máquinas**.

  b. Selecione a guia **Gerenciamento de Energia** e escolha **Sim** para habilitar o gerenciamento de energia para o catálogo de máquinas.

  c. Selecione a conexão apropriada na lista suspensa e clique em **OK**.

Solução de problemas

Escurecimento do monitor não funciona

Se o monitor local do PC Windows não estiver em branco enquanto houver uma sessão HDX ativa (o monitor local exibe o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê ao driver de exibição indireta (IDD) da Citrix uma prioridade maior do que o driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para mais detalhes sobre as prioridades do adaptador de vídeo e a criação de monitores, consulte o artigo do Knowledge Center CTX237608.

A sessão se desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão habilitada

A notificação de gerenciamento de sessão controlada pelo valor de registro **SasNotification** só funciona quando o modo Acesso Remoto para PC está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização habilitados, o PC será relatado como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desabilitará automaticamente o modo Acesso Remoto para PC. Para habilitar o modo Acesso Remoto para PC, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Informações de diagnóstico

As informações de diagnóstico sobre o Acesso Remoto para PC são gravadas no log de Eventos de Aplicativo do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas descartando mensagens duplicadas.

- 3300 (informativo): Máquina adicionada ao catálogo
- 3301 (informativo): Máquina adicionada ao grupo de entrega
- 3302 (informativo): Máquina atribuída ao usuário
- 3303 (erro): Exceção

Gerenciamento de energia

Se o gerenciamento de energia para Acesso Remoto ao 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.

App-V

Usando o App-V com o Citrix Virtual Apps and Desktops™

O Microsoft Application Virtualization (App-V) permite implantar, atualizar e dar suporte a aplicativos como serviços. Os usuários acessam os aplicativos sem instalá-los em seus próprios dispositivos. O App-V e o Microsoft User State Virtualization (USV) fornecem acesso a aplicativos e dados, independentemente do local e da conexão com a internet. A tabela a seguir lista as versões compatíveis.

APP-V	CONTROLADOR DE ENTREGA DO CITRIX VIRTUAL APPS AND DESKTOPS	VDA DO CITRIX VIRTUAL APPS AND DESKTOPS
5.0 e 5.0 SP1	XenDesktop 7 até o atual, XenApp 7.5 até o atual	7.0 até o atual
5.0 SP2	XenDesktop 7 até o atual, XenApp 7.5 até o atual	7.1 até o atual
5.0 SP3 e 5.1	XenDesktop 7.6 até o atual, XenApp 7.6 até o atual	7.6.300 até o atual
App-V no Windows Server 2016	XenDesktop 7.12 até o atual, XenApp 7.12 até o atual	7.12 até o atual

O cliente App-V não oferece suporte ao acesso offline a aplicativos. O suporte à integração do App-V inclui o uso de compartilhamentos SMB para aplicativos. O protocolo HTTP não é compatível. Se você não estiver familiarizado com o App-V, consulte a documentação da Microsoft. Aqui está um resumo dos componentes do App-V mencionados neste artigo:

- **Servidor de gerenciamento**. Fornece um console centralizado para gerenciar a infraestrutura do App-V e entrega aplicativos virtuais para o Cliente de Desktop App-V e para um Cliente de Serviços de Área de Trabalho Remota. O servidor de gerenciamento do App-V autentica, solicita e fornece a segurança, medição, monitoramento e coleta de dados exigidos pelo administrador. O servidor usa o Active Directory e ferramentas de suporte para gerenciar usuários e aplicativos.
- **Servidor de publicação**. Fornece aos clientes App-V aplicativos para usuários específicos e hospeda o pacote de aplicativos virtuais para streaming. Ele busca os pacotes do servidor de gerenciamento.
- **Cliente**. Recupera aplicativos virtuais, publica os aplicativos no cliente e configura e gerencia automaticamente ambientes virtuais em tempo de execução em dispositivos Windows. Você instala o cliente App-V no VDA, onde ele armazena configurações de aplicativos virtuais específicas do usuário, como alterações de registro e arquivo no perfil de cada usuário.

Os aplicativos estão disponíveis de forma transparente, sem qualquer pré-configuração ou alterações nas configurações do sistema operacional. Você pode iniciar aplicativos App-V a partir de Grupos de Entrega de SO de Servidor e SO de Desktop:

- Através do aplicativo Citrix Workspace™
- Através do cliente App-V e do aplicativo Citrix Workspace
- Simultaneamente por vários usuários em vários dispositivos
- Através do Citrix StoreFront™

As propriedades modificadas do aplicativo App-V são implementadas quando o aplicativo é iniciado. Por exemplo, para aplicativos com um nome de exibição modificado ou ícone personalizado, a modificação aparece quando os usuários iniciam o aplicativo. As personalizações de aplicativos salvas em arquivos de configuração dinâmicos também são aplicadas quando o aplicativo é iniciado.

Métodos de gerenciamento

Você pode usar pacotes App-V e arquivos de configuração dinâmicos criados com o sequenciador App-V e, em seguida, localizados em servidores App-V ou compartilhamentos de rede.

- **Servidores App-V:** O uso de aplicativos de pacotes em servidores App-V requer comunicação contínua entre o Studio e os servidores App-V para descoberta, configuração e download para os VDAs. Isso acarreta custos de hardware, infraestrutura e sobrecarga administrativa. O Studio e os servidores App-V devem permanecer sincronizados, principalmente para permissões de usuário.

  Isso é chamado de método de gerenciamento de *administrador duplo* porque o acesso a pacotes e aplicativos App-V requer os consoles do Studio e do servidor App-V. Esse método funciona melhor em implantações App-V e Citrix estreitamente acopladas. Nesse método, o servidor de gerenciamento lida com os arquivos de configuração dinâmica. Ao usar o método de gerenciamento de administrador duplo, os componentes do Citrix App-V gerenciam o registro do servidor de publicação apropriado necessário para o lançamento de um aplicativo. Isso garante que o servidor de publicação seja sincronizado para o usuário no momento apropriado. O servidor de publicação mantém outros aspectos do ciclo de vida do pacote (como atualização no logon e grupos de conexão) usando as configurações com as quais ele está configurado.
- **Compartilhamento de rede:** Pacotes e arquivos de configuração de implantação XML colocados em um compartilhamento de rede removem a dependência do Studio no servidor App-V e na infraestrutura de banco de dados, reduzindo a sobrecarga. (Você deve instalar o cliente Microsoft App-V em cada VDA.)

Isso é chamado de método de gerenciamento de *administrador único* porque o uso de pacotes e aplicativos App-V requer apenas o console do Studio. Você navega até o compartilhamento de rede e adiciona um ou mais pacotes App-V desse local à Biblioteca de Aplicativos no nível do Site . Nesse método, os componentes do Citrix App-V processam os Arquivos de Configuração de Implantação quando o aplicativo é iniciado. (Arquivos de Configuração do Usuário não são suportados.) Ao usar o método de gerenciamento de administrador único, os componentes do Citrix App-V gerenciam todos os aspectos do ciclo de vida do Pacote na máquina host. Os pacotes são adicionados à máquina na inicialização do broker, ou quando uma alteração de configuração é detectada (o que também pode ser no momento do lançamento da sessão). Os pacotes são publicados pela primeira vez para usuários individuais sob demanda 'just in time' quando uma solicitação de lançamento é recebida do aplicativo Citrix Workspace.

O Single Admin também gerencia o ciclo de vida dos grupos de conexão necessários para atender às definições de configuração do Grupo de Isolamento feitas no Studio.

Biblioteca de Aplicativos é um termo Citrix para um repositório de cache que armazena informações sobre pacotes App-V. A Biblioteca de Aplicativos também armazena informações sobre outras tecnologias de entrega de aplicativos Citrix.

Em ambos os métodos de gerenciamento, se o VDA estiver configurado para descartar dados do usuário, a publicação (ou sincronização) deve ser refeita no próximo lançamento da sessão.

Você pode usar um ou ambos os métodos de gerenciamento simultaneamente. Em outras palavras, ao adicionar aplicativos a Grupos de Entrega, os aplicativos podem vir de pacotes App-V localizados em servidores App-V ou em um compartilhamento de rede.

Observação:

Se você estiver usando ambos os métodos de gerenciamento simultaneamente, e o pacote App-V tiver um arquivo de configuração dinâmica em ambos os locais, o arquivo no servidor App-V (gerenciamento duplo) será usado.

Ao selecionar **Configuração > Publicação App-V** no painel de navegação do Studio, a exibição mostra os nomes e as origens dos pacotes App-V. A coluna de origem indica se os pacotes estão localizados no servidor App-V ou armazenados em cache na Biblioteca de Aplicativos. Ao selecionar um pacote, o painel de detalhes lista os aplicativos e atalhos no pacote.

Arquivos de configuração dinâmica

Visão geral

Os pacotes App-V podem ser personalizados usando arquivos de configuração dinâmica que, quando aplicados ao pacote, podem ser usados para alterar suas características. Por exemplo, você pode usá-los para definir atalhos e comportamentos de aplicativos extras. O Citrix App-V suporta ambos os tipos de arquivo de configuração dinâmica. As configurações de arquivo são aplicadas quando o aplicativo é iniciado:

- Os Arquivos de Configuração de Implantação fornecem configuração em toda a máquina para todos os usuários. Espera-se que esses arquivos sejam nomeados \<*packageFileName*>_DeploymentConfig.xml e estejam localizados na mesma pasta que o pacote App-V ao qual se aplicam. Suportado por gerenciamento de administrador único e duplo.
- Os Arquivos de Configuração do Usuário fornecem configuração específica do usuário que suporta personalizações por usuário para o pacote. O Administrador Único suporta arquivos de configuração de usuário nomeados no seguinte formato: \<*packageFileName*>_UserConfig.xml e localizados na mesma pasta que o pacote App-V ao qual se aplicam.

Quando vários arquivos de configuração do usuário existem para um pacote específico, eles são aplicados com a seguinte prioridade:

1. SID do Usuário
2. Nome de usuário
3. SID do Grupo AD (O primeiro encontrado vence)
4. Nome do Grupo AD (O primeiro encontrado vence)
5. Padrão

Por exemplo

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml
```

```
MyAppVPackage_UserConfig.xml
```

Observação:

A parte específica do usuário do nome do arquivo também pode ocorrer opcionalmente no final (por exemplo, MyAppVPackage_UserConfig_**joeblogs**.xml).

Local do arquivo de configuração dinâmica

No gerenciamento de administrador único, os componentes do Citrix App-V processam apenas arquivos de configuração dinâmica que são encontrados na mesma pasta que seu pacote App-V. Quando os aplicativos no pacote são iniciados, quaisquer alterações nos arquivos de configuração dinâmica correspondentes são reaplicadas. Se seus arquivos de configuração dinâmica estiverem localizados em um local diferente de seus pacotes, use um arquivo de mapeamento para mapear pacotes para seus arquivos de configuração de implantação.

Para criar um arquivo de mapeamento

1. Abra um novo arquivo de texto.
2. Para cada arquivo de configuração dinâmica, adicione uma linha que especifique o caminho para o pacote usando o formato \<PackageGuid> : caminho.

   Por exemplo:

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
3. Salve o arquivo como ctxAppVDynamicConfigurations.cfg na mesma pasta do pacote. Toda a hierarquia de diretórios no mesmo compartilhamento UNC do pacote App-V é pesquisada recursivamente para cima por este arquivo toda vez que um aplicativo no pacote é iniciado.

Observação:

Você não pode aplicar alterações à Configuração de Implantação Dinâmica quando há sessões de usuário com um aplicativo do pacote aberto. Você pode aplicar alterações aos arquivos de Configuração Dinâmica do Usuário se outros usuários, *mas não o usuário atual*, tiverem um aplicativo do pacote aberto.

Configurando o IIS para usar arquivos de configuração dinâmica

Os componentes Citrix App-V no VDA podem usar Arquivos de Configuração de Implantação App-V e Arquivos de Configuração de Usuário colocados ao lado do pacote, de acordo com as mesmas regras usadas pelos pacotes hospedados em UNC. Para fazer isso, os componentes do VDA precisam de permissão para navegar na estrutura de diretórios do IIS para determinar qual arquivo usar. Ao contrário dos pacotes hospedados em UNC, o VDA deve primeiro baixar os arquivos de configuração do servidor para um local temporário na máquina host antes que possam ser usados na publicação. Este é um recurso opcional e, se a navegação de diretórios não estiver habilitada, os arquivos de configuração dinâmica serão ignorados.

Execute as seguintes etapas para habilitar a navegação de diretórios para seu site:

1. No console do Gerenciador do IIS, selecione o nó do site e clique duas vezes em **Navegação de Diretórios** no painel central.
2. Clique em **Habilitar** no painel direito e selecione *Hora*, *Tamanho*, *Extensão* e *Data*. (Não selecione Data longa.) Isso permite que os componentes do Citrix App-V no VDA saibam se eles têm as versões mais recentes dos arquivos de configuração aplicadas ou se precisam de atualização.

Grupos de isolamento

Ao usar o método de administrador único do App-V, a criação de grupos de isolamento permite especificar grupos interdependentes de aplicativos que devem ser executados na sandbox. Este recurso é semelhante, mas não idêntico, aos grupos de conexão do App-V. Em vez da terminologia de pacote obrigatório e opcional usada pelo servidor de gerenciamento do App-V, a Citrix usa automático e explícito para as opções de implantação de pacote.

- Quando um usuário inicia um aplicativo App-V (o aplicativo principal), os grupos de isolamento são pesquisados por outros pacotes de aplicativos que estão marcados para inclusão automática. Esses pacotes são baixados e incluídos no grupo de isolamento automaticamente. Você não precisa adicioná-los ao Grupo de Entrega que contém o aplicativo principal.
- Um pacote de aplicativo no grupo de isolamento que está marcado para inclusão explícita é baixado somente se você adicionou explicitamente esse aplicativo ao mesmo Grupo de Entrega que contém o aplicativo principal.

Isso permite criar grupos de isolamento contendo uma mistura de aplicativos incluídos automaticamente que estão disponíveis globalmente para todos os usuários. Além disso, o grupo pode conter um conjunto de plug-ins e outros aplicativos (que podem ter restrições de

licenciamento específicas), que você pode limitar a um determinado conjunto de usuários (identificados por meio de Grupos de Entrega) sem ter que criar mais grupos de isolamento.

Por exemplo, o aplicativo "app-a" requer JRE 1.7 para ser executado. Você pode criar um grupo de isolamento contendo app-a (com um tipo de implantação explícito) e JRE 1.7 (com um tipo de implantação automático). Em seguida, adicione esses pacotes App-V a um ou mais Grupos de Entrega. Quando um usuário inicia app-a, o JRE 1.7 é implantado automaticamente com ele.

Você pode adicionar um aplicativo a mais de um grupo de isolamento App-V. No entanto, quando um usuário inicia esse aplicativo, o primeiro grupo de isolamento ao qual esse aplicativo foi adicionado é sempre usado. Você não pode ordenar ou priorizar outros grupos de isolamento que contenham esse aplicativo.

Balanceamento de carga de servidores App-V

O balanceamento de carga de servidores de gerenciamento e publicação usando DNS Round-Robin é suportado se você estiver usando o método de gerenciamento de administrador duplo. O balanceamento de carga do servidor de gerenciamento atrás de um IP Virtual Netscaler, F5 (ou similar) não é suportado devido à forma como o Studio precisa se comunicar com o Servidor de Gerenciamento via PowerShell remoto. Para obter mais informações, consulte este artigo do blog da Citrix.

Configurando o IIS para hospedar e transmitir pacotes App-V

Para permitir que seu servidor IIS hospede e transmita pacotes App-V, execute as seguintes etapas:

1. Abra o console do Gerenciador do IIS. Consulte `<https://docs.microsoft.com/pt-br/previous-versions/iis/6.0-sdk/ms525920(v%3Dvs.90)>` para obter instruções.
2. Clique com o botão direito do mouse na instância do site que você deseja usar e selecione **Adicionar diretório virtual**.
3. Digite um nome de alias e o caminho onde seus pacotes estão fisicamente armazenados em sua rede.
4. Clique duas vezes em **Tipos MIME** no painel central e, em seguida, clique com o botão direito do mouse em qualquer lugar da janela e selecione **Adicionar**.
5. Para a extensão de nome de arquivo tipo `.appv`, selecione Tipo MIME `application/app-v` e clique em **OK**.

Importando pacotes App-V transmitidos por HTTP para o Citrix DaaS™ (anteriormente serviço Citrix Virtual Apps and Desktops)

Nota:

Este recurso é suportado apenas em Virtual Delivery Agents (VDAs) versão 2009 e posteriores. Se aplicativos em pacotes App-V com caminhos HTTP(S) forem adicionados a grupos de entrega com um nível funcional de 2003 ou posterior, eles serão publicados no Citrix DaaS, mas os usuários não poderão iniciá-los do Citrix Cloud a menos que o VDA seja versão 2009 ou posterior. O nível funcional do grupo de entrega é explicado em Criar grupos de entrega.

1. Baixe e instale/descompacte as versões mais recentes do *CVAD Remote PowerShell SDK* e do *Citrix App-V Package Discovery module*. Consulte os SDKs e APIs do Citrix DaaS.
2. Use o Módulo de Descoberta de Pacotes para importar o pacote App-V do seu servidor IIS para o seu Citrix DaaS. Por exemplo:

```
Import-Module <Download
Directory>\Citrix.Cloud.AppLibrary.Admin.v1.psm1

Import-AppVPackageToCloud

–PackagePath "https://My.AppVServer.net/Packages/Notepad++.appv"
```

3. Faça login na sua conta Citrix Cloud™.
4. O pacote é baixado para um local temporário na sua máquina, de onde as informações relevantes são extraídas e carregadas para a Biblioteca de Aplicativos na sua instância do Citrix DaaS.

Configuração

A tabela a seguir resume a sequência de tarefas de configuração para usar o App-V no Citrix Virtual Apps and Desktops usando métodos de gerenciamento de administrador único e duplo.

ADMINISTRADOR ÚNICO	ADMINISTRADOR DUPLO	TAREFA
X	X	Implantar App-V

ADMINISTRADOR ÚNICO	ADMINISTRADOR DUPLO	TAREFA
X	X	Empacotamento e posicionamento
	X	Configurar endereços de servidor App-V no Studio
X	X	Instalar software em máquinas VDA
X		Adicionar pacotes App-V à Biblioteca de Aplicativos
X		Adicionar grupos de isolamento App-V (opcional)
X	X	Adicionar aplicativos App-V a Grupos de Entrega

Implantar Microsoft App-V

Para instruções de implantação do App-V, consulte `<https://docs.microsoft.com/pt-br/microsoft-desktop-optimization-pack/>`.

Opcionalmente, altere as configurações do servidor de publicação App-V. A Citrix recomenda usar os cmdlets do SDK no Controller. Consulte a documentação do SDK para obter detalhes.

- Para visualizar as configurações do servidor de publicação, digite **Get-CtxAppvServerSetting -AppVPublishingServer \<*pubServer*>**.
- Para garantir que os aplicativos App-V sejam iniciados corretamente, digite **Set-CtxAppvServerSetting –UserRefreshonLogon 0**.

Se você usou anteriormente as configurações de política de GPO para gerenciar as configurações do servidor de publicação, as configurações de GPO substituem quaisquer configurações de integração do App-V, incluindo as configurações de cmdlet. Isso pode resultar em falha no lançamento do aplicativo App-V. A Citrix recomenda que você remova todas as configurações de política de GPO e, em seguida, use o SDK para configurar essas configurações.

Empacotamento e posicionamento

Para qualquer método de gerenciamento, crie pacotes de aplicativos usando o sequenciador App-V. Consulte a documentação da Microsoft para obter detalhes.

- Para gerenciamento de administrador único, disponibilize os pacotes e seus arquivos de configuração dinâmica correspondentes em um local de rede compartilhado UNC ou SMB. Certifique-se de que o administrador do Studio que adiciona aplicativos a Delivery Groups tenha pelo menos acesso de leitura a esse local.
- Para gerenciamento de administrador duplo, 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.)

Independentemente de os pacotes estarem no servidor App-V ou em um compartilhamento de rede, certifique-se de que os pacotes tenham as permissões de segurança apropriadas para permitir que o administrador do Studio os acesse. Os compartilhamentos de rede devem ser compartilhados com "Authenticated users" para garantir que tanto o VDA quanto o Studio tenham acesso de leitura por padrão.

Configurar endereços de servidor App-V no Studio

> **Importante:**
>
> A Citrix recomenda usar os cmdlets do PowerShell no Controller para especificar endereços de servidor App-V se esses servidores usarem valores de propriedade não padrão. Consulte a documentação do SDK para obter detalhes. Se você alterar os endereços do servidor App-V no Studio, algumas propriedades de conexão do servidor que você especificar podem ser redefinidas para valores padrão. Essas propriedades são usadas nos VDAs para se conectar aos servidores de publicação App-V. Se isso acontecer, reconfigure os valores não padrão para quaisquer propriedades redefinidas nos servidores.
>
> Este procedimento é válido apenas para o método de gerenciamento de administrador duplo.

Especifique os endereços do servidor de gerenciamento e publicação do App-V para o método de gerenciamento de administrador duplo durante ou após a criação do Site. Você pode fazer isso durante ou após a criação do Site.

Durante a criação do Site:

- Na página **App-V** do assistente, insira o URL do servidor de gerenciamento do Microsoft App-V e o URL e o número da porta do servidor de publicação do App-V.

- Teste a conexão antes de continuar com o assistente. Se o teste falhar, consulte a seção Solução de problemas abaixo.

Após a criação do Site:

1. Selecione **Configuração > Publicação do App-V** no painel de navegação do Studio.
2. Se você não especificou endereços de servidor App-V anteriormente, selecione **Adicionar Servidor Microsoft** no painel Ações.
3. Para alterar os endereços do servidor App-V, selecione **Editar Servidor Microsoft** no painel Ações.
4. Insira o URL do servidor de gerenciamento do Microsoft App-V e o URL e o número da porta do servidor de publicação do App-V.
5. Teste a conexão com esses servidores antes de fechar a caixa de diálogo. Se o teste falhar, consulte a seção Solução de problemas abaixo.

Mais tarde, se você quiser remover todos os links para os servidores de gerenciamento e publicação do App-V e impedir que o Studio descubra pacotes App-V desses servidores, selecione **Remover Servidor Microsoft** no painel Ações. Esta ação é permitida somente se nenhum aplicativo em pacotes nesses servidores estiver atualmente publicado em quaisquer Grupos de Entrega. Se estiverem, você deve remover esses aplicativos dos Grupos de Entrega antes de poder remover os servidores App-V.

Instalar software em máquinas VDA

As máquinas que contêm VDAs devem ter dois conjuntos de software instalados para suportar o App-V: um da Microsoft e outro da Citrix.

Cliente Microsoft App-V

Este software recupera aplicativos virtuais, publica os aplicativos no cliente e configura e gerencia automaticamente ambientes virtuais em tempo de execução em dispositivos Windows. O cliente App-V armazena configurações de aplicativos virtuais específicas do usuário, como alterações de registro e arquivo no perfil de cada usuário.

O cliente App-V está disponível na Microsoft. Instale um cliente em cada máquina que contém um VDA, ou na imagem mestre que é usada em um catálogo de máquinas para criar VMs. **Nota**: Windows 10 (1607 ou superior) e Windows Server 2016 já incluem o cliente App-V. Somente nesses sistemas operacionais, habilite o cliente App-V executando o cmdlet PowerShell **Enable-AppV** (sem parâmetros). O cmdlet **Get-AppVStatus** recupera o status de habilitação atual.

> **Dica:**

> Depois de instalar o cliente App-V, com permissões de Administrador, execute o cmdlet PowerShell **Get-AppvClientConfiguration** e certifique-se de que EnablePackageScripts esteja definido como 1. Se não estiver definido como 1, execute **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Componentes Citrix App-V

O software do componente Citrix App-V é excluído por padrão ao instalar um VDA.

Você pode controlar este comportamento padrão durante a instalação do VDA. Na interface gráfica, selecione a caixa de seleção **Citrix Personalization for App-V - VDA** na página **Componentes Adicionais**. Na interface de linha de comando, use a opção **/includeadditional "Citrix Personalization for App-V – VDA"**.

Se você não incluir os componentes Citrix App-V durante a instalação do VDA, mas depois quiser usar aplicativos App-V: Na lista Programas e Recursos da máquina Windows, clique com o botão direito na entrada **Citrix Virtual Delivery Agent** e selecione **Alterar**. Um assistente será iniciado. No assistente, ative a opção que instala e habilita os componentes de publicação do App-V.

Adicionar ou remover pacotes App-V na Biblioteca de Aplicativos

Esses procedimentos são válidos apenas para o método de gerenciamento de administrador único.

Você deve ter pelo menos acesso de leitura ao compartilhamento de rede que contém os pacotes App-V.

Adicionar um pacote App-V à Biblioteca de Aplicativos

1. Selecione **Configuração > Publicação App-V** no painel de navegação do Studio.
2. Selecione **Adicionar Pacotes** no painel Ações.
3. Navegue até o compartilhamento que contém os pacotes App-V e selecione um ou mais pacotes.
4. Clique em **Adicionar**.

Remover um pacote App-V da Biblioteca de Aplicativos

A remoção de um pacote App-V da Biblioteca de Aplicativos o remove da exibição do nó de Publicação App-V do Studio. No entanto, isso não remove seus aplicativos dos Grupos de

Entrega, e esses aplicativos ainda podem ser iniciados. O pacote permanece em seu local de rede físico. (Este efeito difere da remoção de um aplicativo App-V de um Grupo de Entrega.)

1. Selecione **Configuração > Publicação App-V** no painel de navegação do Studio.
2. Selecione um ou mais pacotes a serem removidos.
3. Selecione **Remover Pacote** no painel Ações.

Adicionar, editar ou remover grupos de isolamento do App-V

Adicionar um grupo de isolamento do App-V

1. Selecione **Publicação do App-V** no painel de navegação do Studio.
2. Selecione **Adicionar Grupo de Isolamento** no painel Ações.
3. Na caixa de diálogo **Configurações de Adição de Grupo de Isolamento**, digite um nome e uma descrição para o grupo de isolamento.
4. Na lista Pacotes Disponíveis, selecione os aplicativos que deseja adicionar ao grupo de isolamento e clique na seta para a direita. Os aplicativos selecionados devem agora aparecer na lista Pacotes no Grupo de Isolamento. No menu suspenso **Implantação** ao lado de cada aplicativo, selecione **Explícito** ou **Automático**. Você também pode usar as setas para cima e para baixo para alterar a ordem dos aplicativos na lista.
5. Quando terminar, clique em **OK**.

Editar um grupo de isolamento do App-V

1. Selecione **Publicação do App-V** no painel de navegação do Studio.
2. Selecione a guia **Grupos de Isolamento** no painel central e selecione o grupo de isolamento que deseja editar.
3. Selecione **Editar Grupo de Isolamento** no painel Ações.
4. Na caixa de diálogo **Configurações de Edição de Grupo de Isolamento**, altere o nome ou a descrição do grupo de isolamento, adicione ou remova aplicativos, altere o tipo de implantação ou altere a ordem dos aplicativos.
5. Quando terminar, clique em **OK**.

Remover um grupo de isolamento do App-V

Remover um grupo de isolamento não remove os pacotes de aplicativos. Ele remove apenas o agrupamento.

1. Selecione **Publicação App-V** no painel de navegação do Studio.

2. Selecione a guia **Grupos de Isolamento** no painel central e, em seguida, selecione o grupo de isolamento que deseja remover.
3. Selecione **Remover Grupo de Isolamento** no painel Ações.
4. Confirme a remoção.

Adicionar aplicativos App-V a Grupos de Entrega

O procedimento a seguir foca em como adicionar aplicativos App-V a Grupos de Entrega. Para detalhes completos sobre a criação de um Grupo de Entrega, consulte Criar Grupos de Entrega.

Etapa 1: Escolha se deseja criar um novo Grupo de Entrega ou adicionar aplicativos App-V a um Grupo de Entrega existente:

Para criar um Grupo de Entrega contendo aplicativos App-V:

1. Selecione **Grupos de Entrega** no painel de navegação do Studio.
2. Selecione **Criar Grupo de Entrega** no painel Ações.
3. Nas páginas sucessivas do assistente, especifique um catálogo de máquinas e usuários.

Para adicionar aplicativos App-V a Grupos de Entrega existentes:

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione **Adicionar Aplicativos** no painel Ações.
3. Selecione um ou mais Grupos de Entrega onde os aplicativos App-V serão adicionados.

Etapa 2: Na página **Aplicativos** do assistente, clique na lista suspensa **Adicionar** para exibir as fontes de aplicativos. Selecione **App-V**.

Etapa 3: Na página **Adicionar Aplicativos App-V**, escolha a fonte App-V: o servidor App-V ou a Biblioteca de Aplicativos. A exibição resultante inclui os nomes dos aplicativos, além de seus nomes de pacote e versões de pacote. Marque as caixas de seleção ao lado dos aplicativos ou atalhos de aplicativo que você deseja adicionar. Em seguida, clique em **OK**.

Etapa 4: Conclua o assistente.

É bom saber:

- Se você alterar as propriedades de um aplicativo App-V ao adicioná-lo a um Grupo de Entrega, as alterações serão feitas quando o aplicativo for iniciado. Por exemplo, se você modificar o nome de exibição ou o ícone de um aplicativo ao adicioná-lo ao grupo, a alteração aparecerá quando um usuário iniciar o aplicativo.

- Se você usar arquivos de configuração dinâmica para personalizar as propriedades de um aplicativo App-V, essas propriedades substituirão quaisquer alterações feitas ao adicioná-los a um Grupo de Entrega.
- Se você editar posteriormente um Grupo de Entrega contendo aplicativos App-V, não haverá alteração no desempenho do aplicativo App-V se você alterar o tipo de entrega do grupo de desktops e aplicativos para apenas aplicativos.
- Ao remover um pacote App-V publicado anteriormente (administrador único) de um Grupo de Entrega, os componentes do cliente Citrix App-V tentam limpar, cancelar a publicação e remover quaisquer pacotes que não estejam mais em uso pelo método de gerenciamento de administrador único.
- Se você estiver usando uma implantação híbrida — com pacotes entregues pelo método de gerenciamento de administrador único e um servidor de publicação App-V, gerenciado por administrador duplo ou por outro mecanismo (como política de grupo) — não é possível determinar quais pacotes (agora potencialmente redundantes) vieram de qual fonte. Neste caso, a limpeza não é tentada.
- Se você publicar mais de 100 aplicativos App-V em um único Grupo de Entrega, os aplicativos podem não ser iniciados. Se isso ocorrer, use a propriedade MaxReceivedMessageSize no elemento de ligação apropriado para aumentar o tamanho máximo da mensagem recebível na configuração do Delivery Controller e/ou do Broker Agent no VDA.

Solução de problemas

Problemas que podem ocorrer apenas ao usar o método de administrador duplo são marcados (DUAL).

(DUAL) Há um erro de conexão do PowerShell ao selecionar **Configuração > Publicação App-V** no painel de navegação do Studio.

- O administrador do Studio também é um administrador do servidor App-V? O administrador do Studio deve pertencer ao grupo "administrators" no servidor de gerenciamento App-V para que possa se comunicar com ele.

(DUAL) A operação Testar conexão retorna um erro ao especificar endereços de servidor App-V no Studio.

- O servidor App-V está ligado? Envie um comando Ping ou verifique o Gerenciador do IIS; cada servidor App-V deve estar no estado Iniciado e Em execução.

- O PowerShell remoting está habilitado no servidor App-V? Caso contrário, consulte `<https://docs.microsoft.com/pt-br/previous-versions/technet-magazine/ff700227(v=msdn.10)>`.
- O administrador do Studio também é um administrador do servidor App-V? O administrador do Studio deve pertencer ao grupo *administrators* no servidor de gerenciamento do App-V para que possa se comunicar com ele.
- O compartilhamento de arquivos está habilitado no servidor App-V? Digite `\\<App-V server FQDN>` no Windows Explorer ou com o comando Executar.
- O servidor App-V tem as mesmas permissões de compartilhamento de arquivos que o administrador do App-V? No servidor App-V, adicione uma entrada para `\\<App-V server FQDN>` em Nomes de Usuário e Senhas Armazenados, especificando as credenciais do usuário que tem privilégios de administrador no servidor App-V. Para obter orientação, consulte `<http://support.microsoft.com/kb/306541>`.
- O servidor App-V está no Active Directory?

  Se a máquina Studio e o servidor App-V estiverem em domínios diferentes do Active Directory que não têm uma relação de confiança, no console do PowerShell na máquina Studio, execute **winrm s winrm/Config/client '@(TrustedHosts="\<*App-V server FQDN*>")'**.

  Se TrustedHosts for gerenciado por GPO, a seguinte mensagem de erro será exibida: "*The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to Not Configured to change the config setting*." Neste caso, adicione uma entrada para o nome do servidor App-V à política TrustedHosts no GPO (Modelos Administrativos > Componentes do Windows > Gerenciamento Remoto do Windows (WinRM) > Cliente WinRM).

(DUAL) A descoberta falha ao adicionar um aplicativo App-V a um Grupo de Entrega.

- O administrador do Studio também é um administrador do servidor de gerenciamento do App-V? O administrador do Studio deve pertencer ao grupo *administrators* no servidor de gerenciamento do App-V para que possa se comunicar com ele.
- O servidor de gerenciamento do App-V está em execução? Envie um comando Ping ou verifique o Gerenciador do IIS; cada servidor App-V deve estar no estado Iniciado e Em Execução.
- O PowerShell remoting está habilitado em ambos os servidores App-V? Caso contrário, consulte `<https://docs.microsoft.com/pt-br/previous-versions/technet-magazine/ff700227(v=msdn.10)>`.

- Os pacotes têm as permissões de segurança apropriadas para o administrador do Studio acessar?

Aplicativos App-V são iniciados apenas em uma versão do navegador.

- Se você publicar várias versões sequenciadas do mesmo aplicativo de navegador, apenas uma versão do aplicativo poderá ser iniciada por vez por usuário no VDA. O mesmo ocorre mesmo que os componentes Citrix não estejam envolvidos e o usuário inicie os aplicativos sequenciados a partir de atalhos da área de trabalho que apontam para caminhos diferentes.

  Qualquer versão do navegador que um usuário iniciar primeiro, determinará a versão do navegador que será executada subsequentemente para ele. Quando o Firefox detecta um segundo lançamento de si mesmo, ele prefere criar uma instância do processo já em execução, em vez de criar um novo processo. Outros navegadores podem se comportar da mesma maneira.

  Você pode fazer com que o aplicativo seja iniciado na versão pretendida do navegador Firefox, adicionando o parâmetro de linha de comando **-no-remote** ao comando de inicialização do atalho. Outros navegadores oferecem o mesmo recurso ou um recurso semelhante.

  > **Nota:**
  >
  > Você deve estar usando o XenApp 7.17 ou superior para aproveitar o recurso de enumeração de atalhos. Você também deve alterar o pacote em ambas as versões do aplicativo para obter esse comportamento bidirecional.

Aplicativos App-V não são iniciados.

- (DUAL) O servidor de publicação está em execução?
- (DUAL) Os pacotes App-V têm permissões de segurança apropriadas para que os usuários possam acessá-los?
- (DUAL) No VDA, certifique-se de que Temp esteja apontando para o local correto e que haja espaço suficiente disponível no diretório Temp.
- (DUAL) No servidor de publicação App-V, execute `Get-AppvPublishingServer *` para exibir a lista de servidores de publicação.
- (DUAL) No servidor de publicação App-V, certifique-se de que UserRefreshonLogon esteja definido como False.

- (DUAL) No servidor de publicação App-V, como administrador, execute **Set-AppvPublishingServer** e defina UserRefreshonLogon como False.
- Uma versão compatível do cliente App-V está instalada no VDA? O VDA tem a configuração **enable package scripts** ativada?
- Na máquina que contém o cliente App-V e o VDA, no Editor do Registro (regedit), vá para HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Certifique-se de que a chave AppVServers tenha o seguinte formato de valor: AppVManagementServer+metadata;PublishingServer (por exemplo: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082)`.
- Na máquina ou imagem mestre que contém o cliente App-V e o VDA, verifique se o PowerShell ExecutionPolicy está definido como RemoteSigned. O cliente App-V fornecido pela Microsoft não é assinado, e este ExecutionPolicy permite que o PowerShell execute scripts e cmdlets locais não assinados. Use um dos dois métodos a seguir para definir o ExecutionPolicy: (1) Como administrador, insira o cmdlet: **Set-ExecutionPolicy RemoteSigned**, ou (2) Nas configurações de Política de Grupo, vá para Configuração do Computador > Políticas > Modelos Administrativos > Componentes do Windows > Windows PowerShell > Ativar Execução de Script.
- Se o erro "RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register" aparecer, use a propriedade MaxReceivedMessageSize no elemento de ligação apropriado para aumentar o tamanho máximo da mensagem recebível na configuração do Delivery Controller e/ou do Broker Agent no VDA.

Se essas etapas não resolverem os problemas, ative e examine os logs.

Logs

Os logs relacionados à configuração do App-V estão localizados em C:\CtxAppvLogs. Os logs de inicialização do aplicativo estão localizados em: %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA resolve para a pasta local do usuário logado. Verifique a pasta local do usuário para quem a inicialização do aplicativo falhou.

Para habilitar os logs do Studio e VDA usados para App-V, você deve ter privilégios de administrador. Você também precisará de um editor de texto como o Bloco de Notas.

Para habilitar os logs do Studio:

1. Crie a pasta C:\CtxAppvLogs.

2. Vá para C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Abra CtxAppvCommon.dll.config em um editor de texto e descomente a linha: \<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. Reinicie o serviço Broker para iniciar o registro.

Para habilitar os logs do VDA:

1. Crie a pasta C:\CtxAppvLogs.
2. Vá para C:\Program Files\Citrix\ Virtual Desktop Agent. Abra CtxAppvCommon.dll.config em um editor de texto e descomente a seguinte linha: \<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. Descomente a linha e defina o campo de valor como 1: \<add key ="EnableLauncherLogs" value="1"/>
4. Reinicie a máquina para iniciar o registro.

Publicar conteúdo

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 deve 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. Não é possível usar o Studio para publicar conteúdo. No entanto, você pode usar o 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* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Se você estiver usando o Citrix DaaS, autenticar inserindo suas credenciais do Citrix Cloud™. Se houver mais de um cliente, escolha um.

Publicar uma URL

Após atribuir o local e o nome do aplicativo, o cmdlet a seguir publica a página inicial da Citrix® como um aplicativo.

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

Verificar o 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 como personalizar o ícone, consulte `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`.
- Clique no aplicativo **Citrix Home Page**. A URL é iniciada em uma nova guia em uma instância local do seu navegador padrão.

Publicar recursos localizados em caminhos UNC

Neste exemplo, o administrador já criou um compartilhamento chamado `PublishedResources`. Após atribuir os locais e nomes 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
```

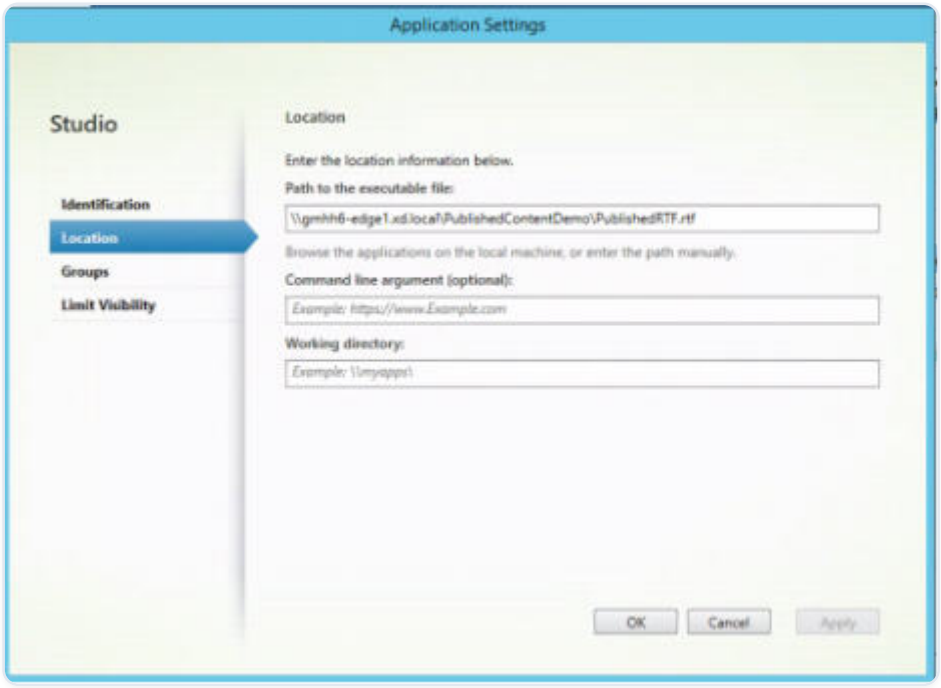
Verificar sucesso:

- 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

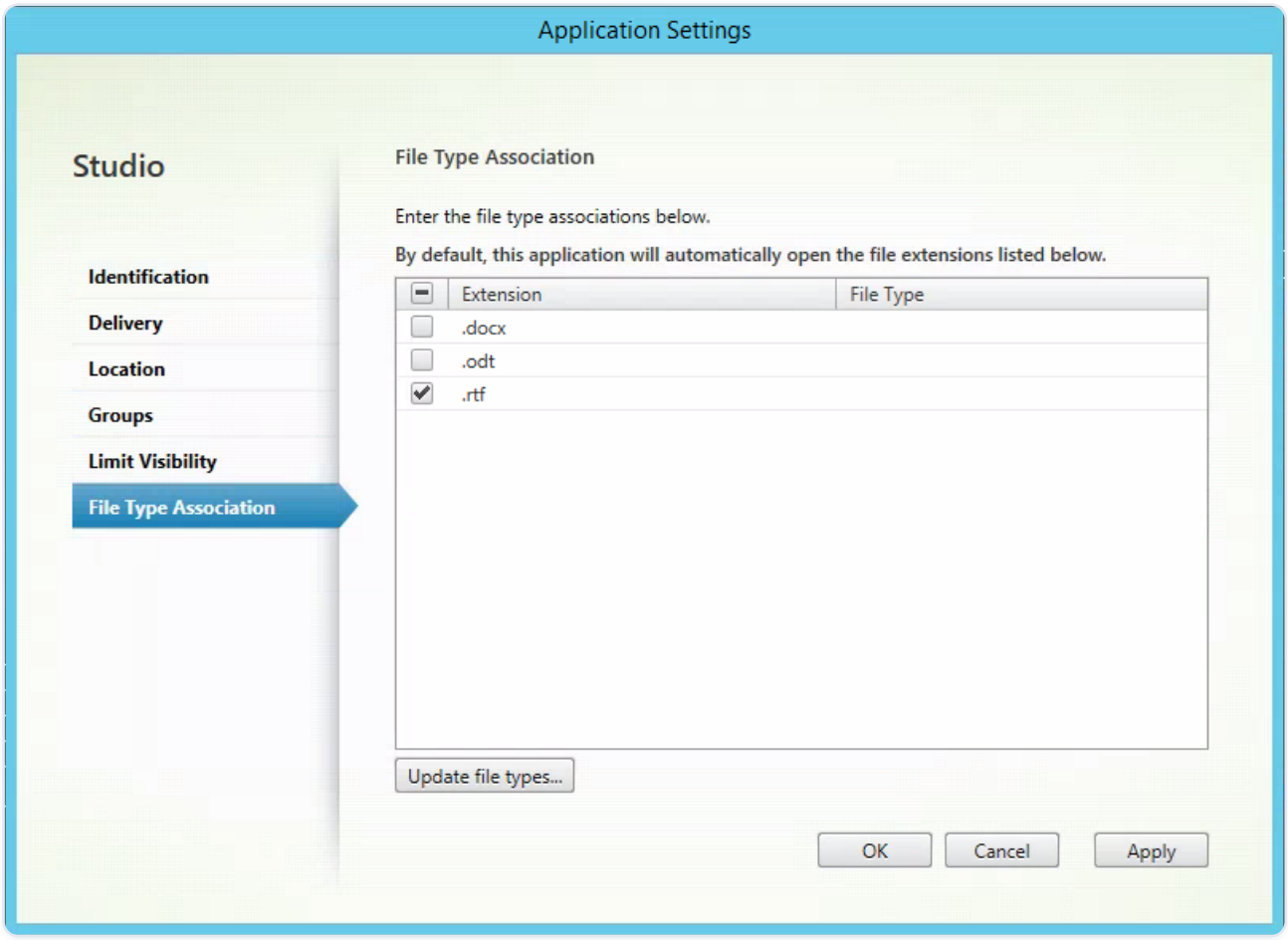
Você gerencia o conteúdo publicado usando os mesmos métodos que usa para outros tipos de aplicativo. Os itens de conteúdo publicado aparecem na lista **Aplicativos** no Studio e podem ser editados no Studio.

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**. Para alterar o recurso, modifique o campo **Caminho para o arquivo executável** nessa página.

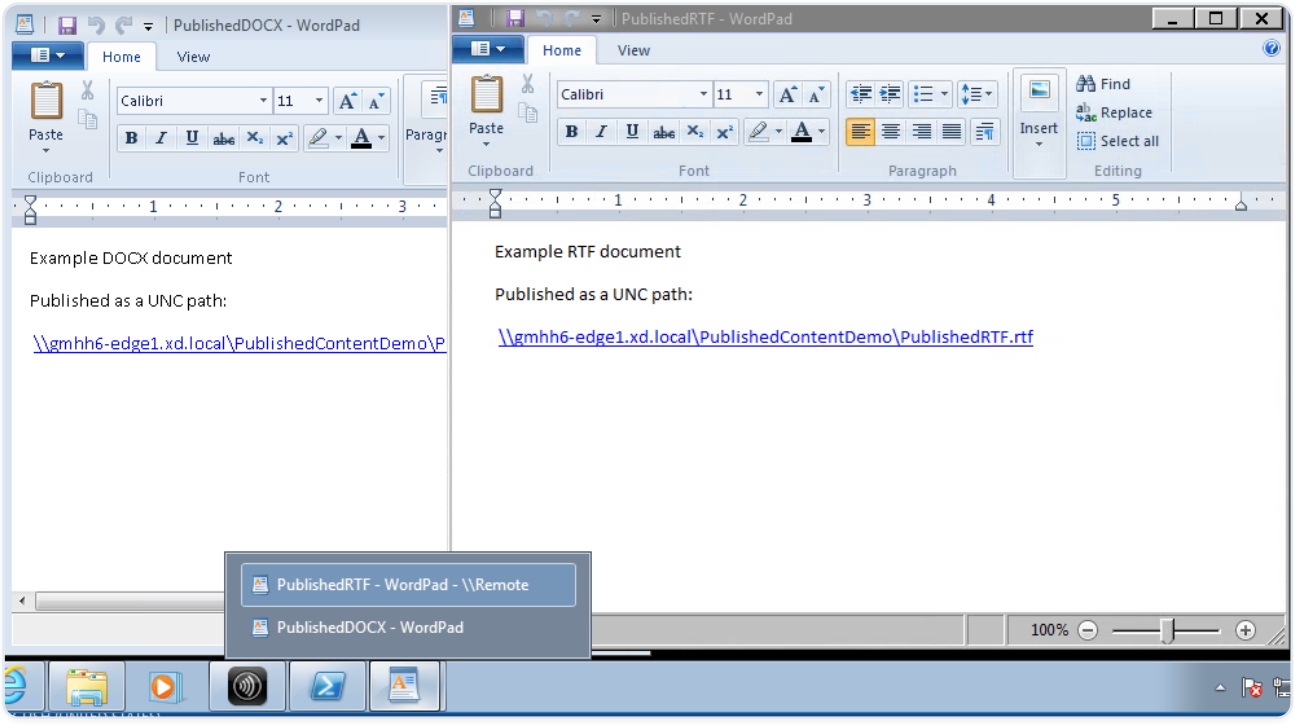


Para usar um aplicativo publicado para abrir um aplicativo `PublishedContent` (em vez de um aplicativo local), edite a propriedade **Associação de Tipo de Arquivo** do aplicativo publicado. Neste exemplo, o aplicativo WordPad publicado foi editado para criar uma Associação de Tipo de Arquivo para arquivos .rtf.

Ative o modo de manutenção para o grupo de entrega antes de editar a Associação de Tipo de Arquivo. Lembre-se de desativar o modo de manutenção quando terminar.



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

VDI de Servidor

Use o recurso Server VDI (Virtual Desktop Infrastructure) para entregar um desktop a partir 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 compatível com 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 VDI de Servidor

1. Prepare o servidor Windows para a instalação.
   - Use o Gerenciador de Servidores do 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 mestre 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 você estiver instalando o VDA em uma imagem e usará o MCS para criar VMs de servidor a partir dessa imagem.
   - Para todos os detalhes da opção, 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 posteriormente. Para obter detalhes, consulte Registro de VDA.

Camada de personalização do usuário

O recurso de camada de personalização do usuário para Citrix Virtual Apps and Desktops™ estende os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e os aplicativos instalados localmente entre as sessões. Alimentado pela tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e ao Machine Creation Services (MCS) em um catálogo de máquinas não persistente.

Você instala os componentes da camada de personalização do usuário juntamente com o Virtual Delivery Agent dentro da imagem mestre. Um arquivo VHD armazena localmente os aplicativos instalados pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

Importante:

Você pode implantar camadas de personalização do usuário no Citrix Virtual Apps and Desktops, ou camadas de usuário do App Layering habilitadas em um modelo de imagem, mas não ambos. Não instale o recurso de camada de personalização do usuário em uma camada dentro do App Layering.

Este recurso substitui o Personal vDisk (PvD), ao mesmo tempo em que oferece uma experiência de espaço de trabalho persistente para os usuários em um ambiente de desktop não persistente e agrupado.

Para implantar o recurso de camada de personalização do usuário, instale e configure-o usando as etapas detalhadas no artigo. Até então, o recurso não está disponível.

Suporte a aplicativos

Além das seguintes exceções, todos os aplicativos que um usuário instala localmente na área de trabalho são suportados na camada de personalização do usuário.

Exceções

Os seguintes aplicativos são a exceção e não são suportados na camada de personalização do usuário:

- Aplicativos corporativos, como MS Office e Visual Studio.
- Aplicativos que modificam a pilha de rede ou hardware. Exemplo: um cliente VPN.
- Aplicativos que possuem drivers de nível de inicialização. Exemplo: um scanner de vírus.
- Aplicativos com drivers que usam o armazenamento de drivers. Exemplo: um driver de impressora.

> **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 persistirão 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
- Citrix Provisioning™, versão 1909 ou posterior
- Compartilhamento de Arquivos do Windows (SMB) ou Azure Files com autenticação AD local habilitada

Você pode implantar o recurso de camada de personalização do usuário nas seguintes versões do Windows quando o SO é implantado como sessão única. O suporte é limitado a um único usuário em uma única sessão.

- Windows 10 Enterprise x64, versão 1607 ou posterior
- Windows 10 Multi-Session (Azure Files suportado)
- Windows Server 2016 (Azure Files suportado)
- Windows Server 2019 (Azure Files suportado)

Para Citrix Virtual Apps and Desktops 7, o uso de Azure Files com camadas de personalização do usuário é suportado no Windows Server 2019, Windows Server 2016v e cliente Windows 10.

> **Nota:**

> A camada de personalização do usuário é suportada apenas como uma implantação de VDI de Servidor. Para obter detalhes da 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 funciona apenas com desktops não persistentes.

> Desinstale o recurso de camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

Configure seu compartilhamento de arquivos

O recurso de camada de personalização do usuário requer armazenamento Windows Server Message Block (SMB). Para criar um compartilhamento de arquivos do Windows, siga as etapas usuais para o sistema operacional Windows que você está usando.

Para saber mais sobre como usar o Azure Files com catálogos baseados em Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

Recomendações

Siga as recomendações nesta seção para uma implantação bem-sucedida da camada de personalização do usuário.

Solução de Gerenciamento de Perfil

A camada de personalização do usuário armazena todas as alterações que o usuário faz para uma única imagem de catálogo de máquina. Para adicionar recursos aprimorados, como dados de perfil móvel em várias imagens de catálogo, a Citrix recomenda também usar o Profile Management. Consulte a documentação do Profile Management para obter mais detalhes.

Ao usar o Profile Management com o recurso de camada de personalização do usuário, limpe a exclusão das informações do usuário no logoff. Você pode limpar a exclusão usando um Objeto de Política de Grupo (GPO) ou a política no Delivery Controller™ (DDC).

Para detalhes sobre as políticas de Profile Management disponíveis, consulte Descrições e padrões de políticas de Profile Management.

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 thin-provisioned 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, você pode inserir um valor diferente para a política do Studio **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 Studio. Em seguida, você atribui as políticas ao grupo de entrega vinculado ao catálogo de máquinas, onde o recurso é implantado.

Se você deixar a imagem mestre sem configuração de camada de personalização do usuário, os serviços permanecerão ociosos e não interferirão nas atividades de autoria.

Se você definir as políticas na imagem mestre, os serviços tentarão executar e montar uma camada de usuário dentro da imagem mestre. A imagem mestre exibirá comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, conclua as seguintes etapas nesta ordem:

- Etapa 1: Verificar a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Etapa 2: Preparar sua imagem mestre.
- Etapa 3: Criar um catálogo de máquinas.

- Passo 4: Crie um grupo de entrega.
- Passo 5: Crie políticas personalizadas de grupo de entrega.

Passo 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

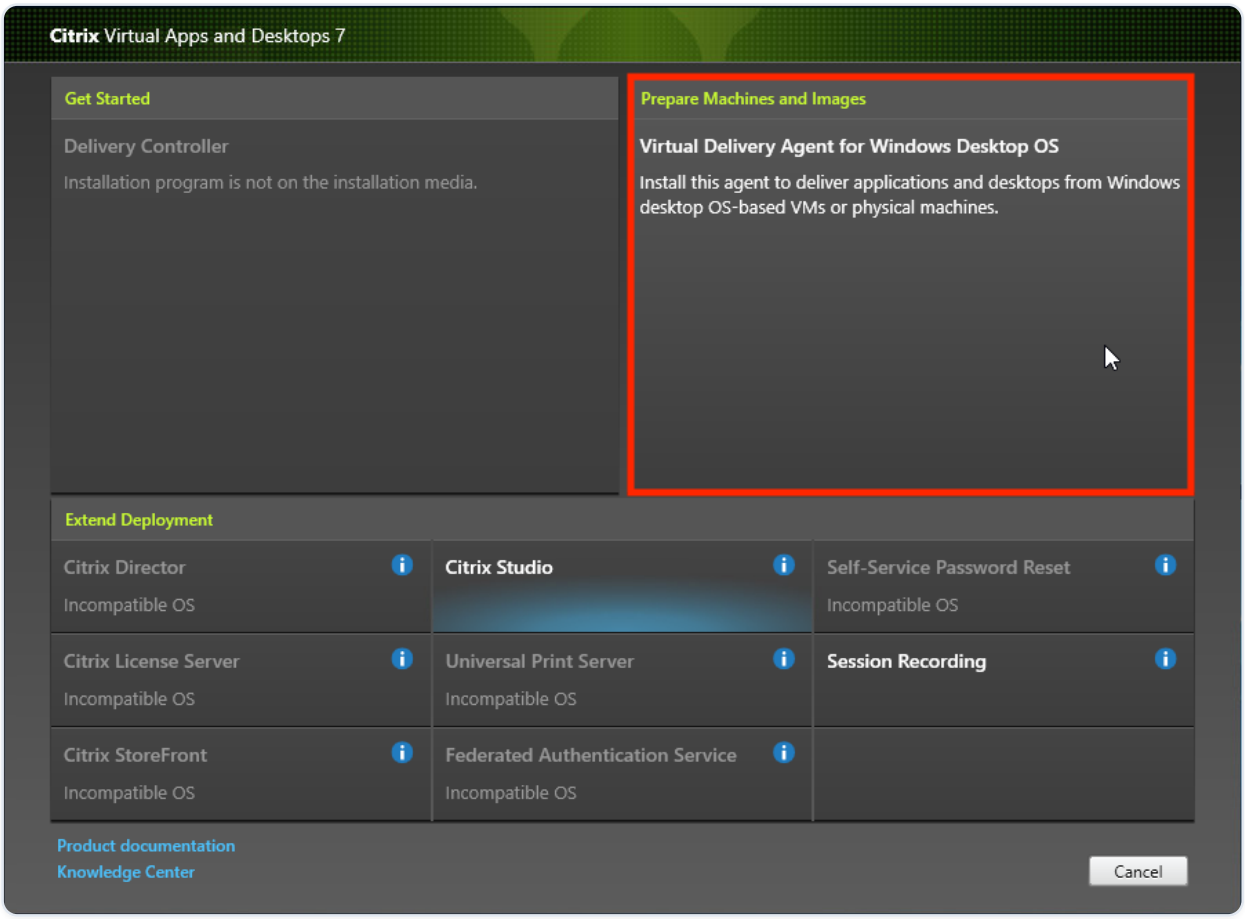
Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops esteja disponível para uso com este novo recurso. Para obter detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

Passo 2: Prepare sua imagem mestre

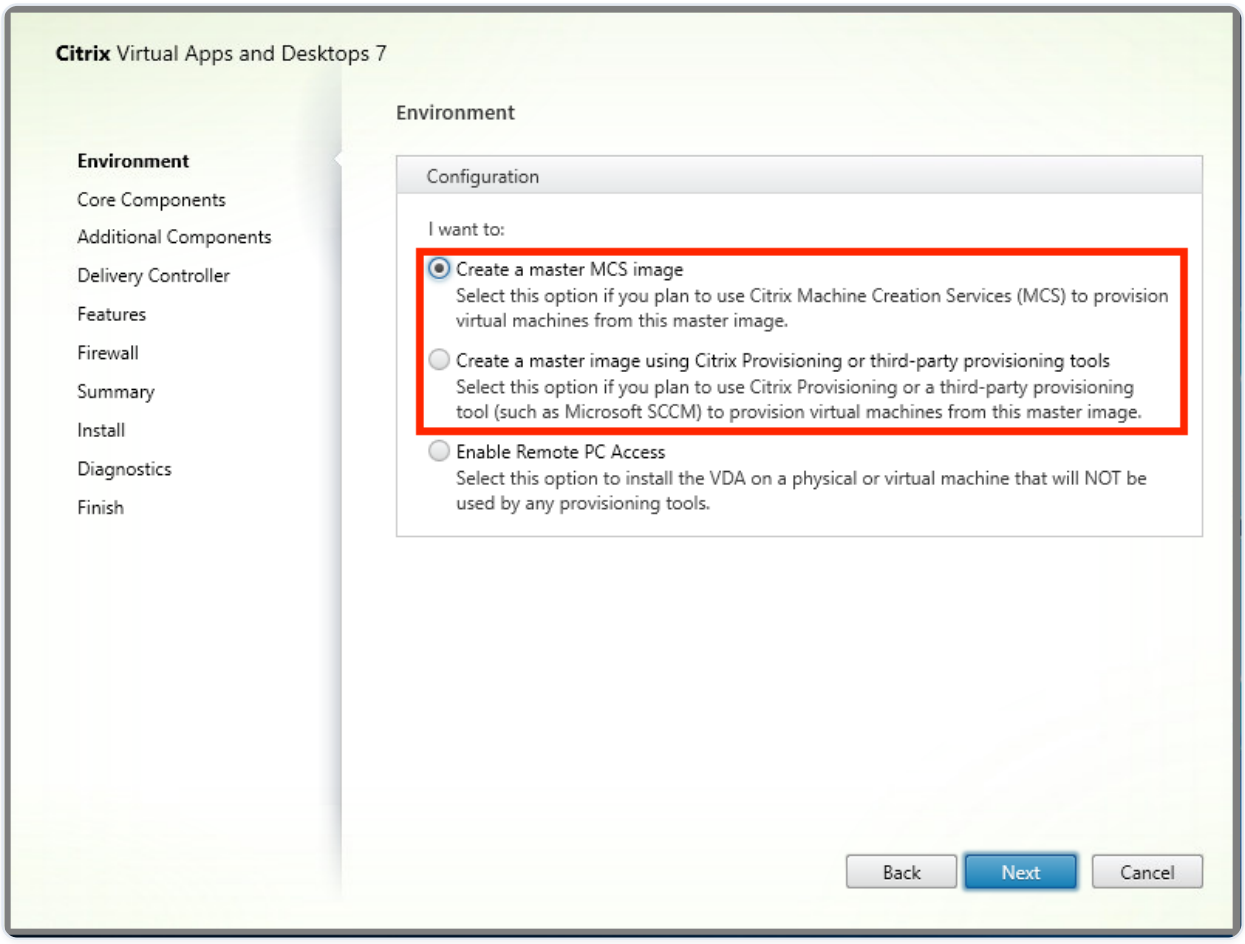
Para preparar sua imagem mestre:

1. Localize a imagem mestre. Instale os aplicativos corporativos da sua organização e quaisquer outros aplicativos que seus usuários geralmente considerem úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Certifique-se de incluir o componente opcional, a **camada de personalização do usuário**. Para obter detalhes, consulte as Opções de linha de comando para instalar um VDA.
3. Se você estiver usando o Windows 10, instale o Virtual Delivery Agent (VDA) 1912. Se uma versão mais antiga do VDA já estiver instalada, desinstale a versão antiga primeiro. Ao instalar a nova versão, certifique-se de selecionar e instalar o componente opcional, a **Camada de Personalização do Usuário Citrix**, da seguinte forma:

    a. Clique no bloco, **Virtual Delivery Agent para SO de Desktop Windows**:

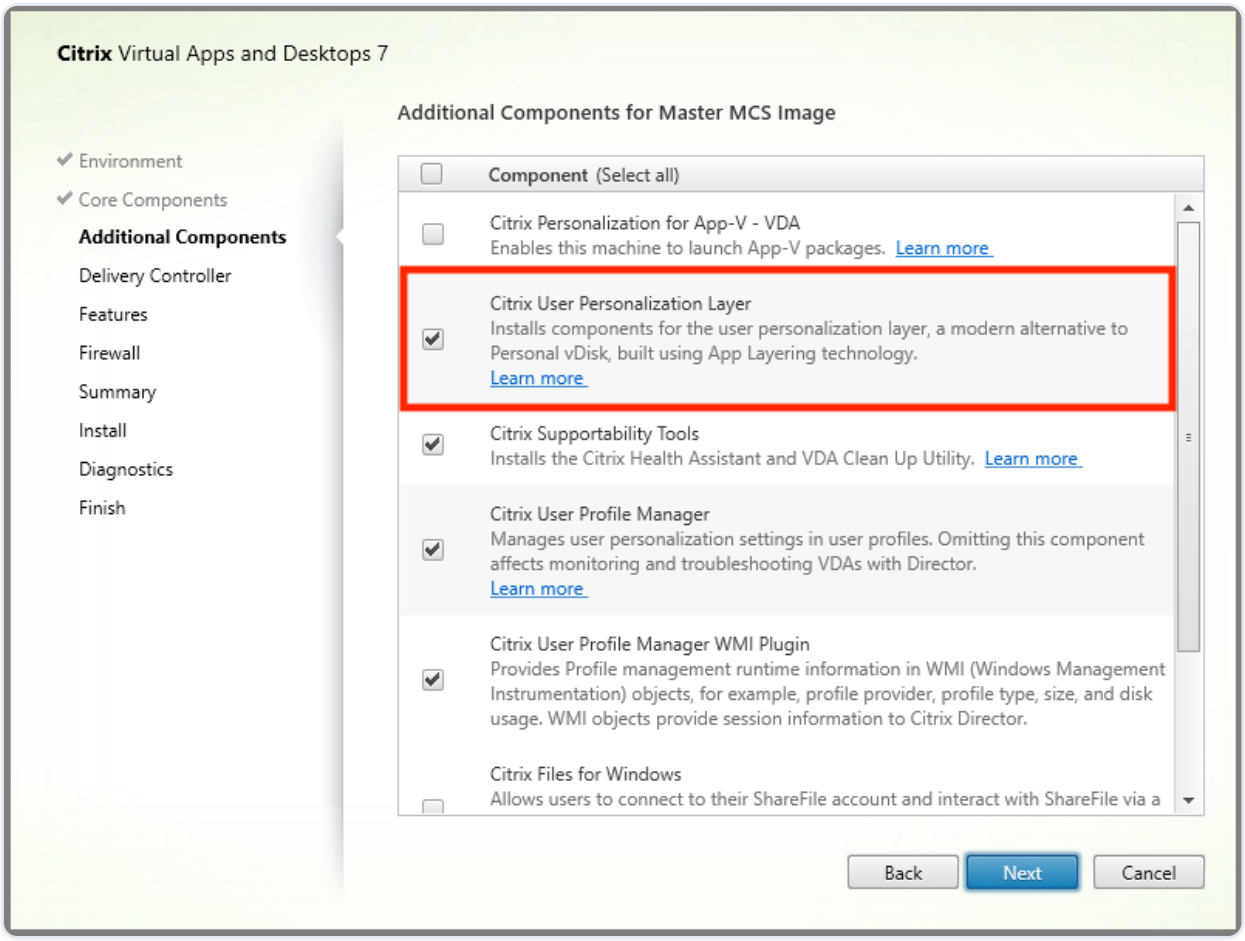


a. **Ambiente:** Selecione Criar uma imagem mestre MCS ou Criar uma imagem mestre usando o Citrix Provisioning ou ferramentas de provisionamento de terceiros.



a. **Componentes Principais:** Clique em **Avançar**.

b. **Componentes Adicionais:** Marque **Camada de Personalização do Usuário Citrix**.



a. Clique nas telas de instalação restantes, configurando o VDA conforme necessário, e clique em Instalar. A imagem reinicia uma ou mais vezes durante a instalação.

4. Deixe as **atualizações do Windows** desabilitadas. O instalador da camada de personalização do usuário desabilita as atualizações do Windows na imagem. Deixe as atualizações desabilitadas.

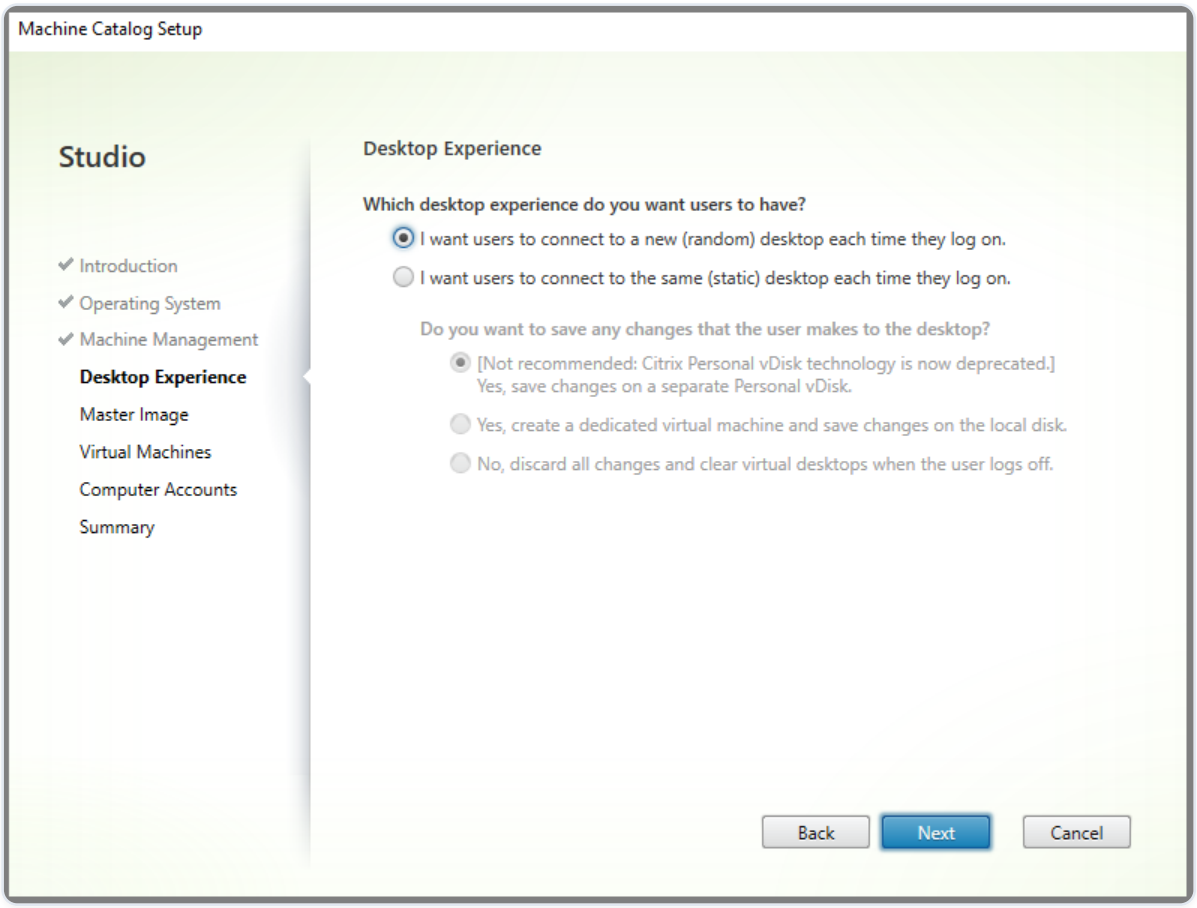
A imagem está pronta para ser carregada no Studio.

Etapa 3: Criar um catálogo de máquinas

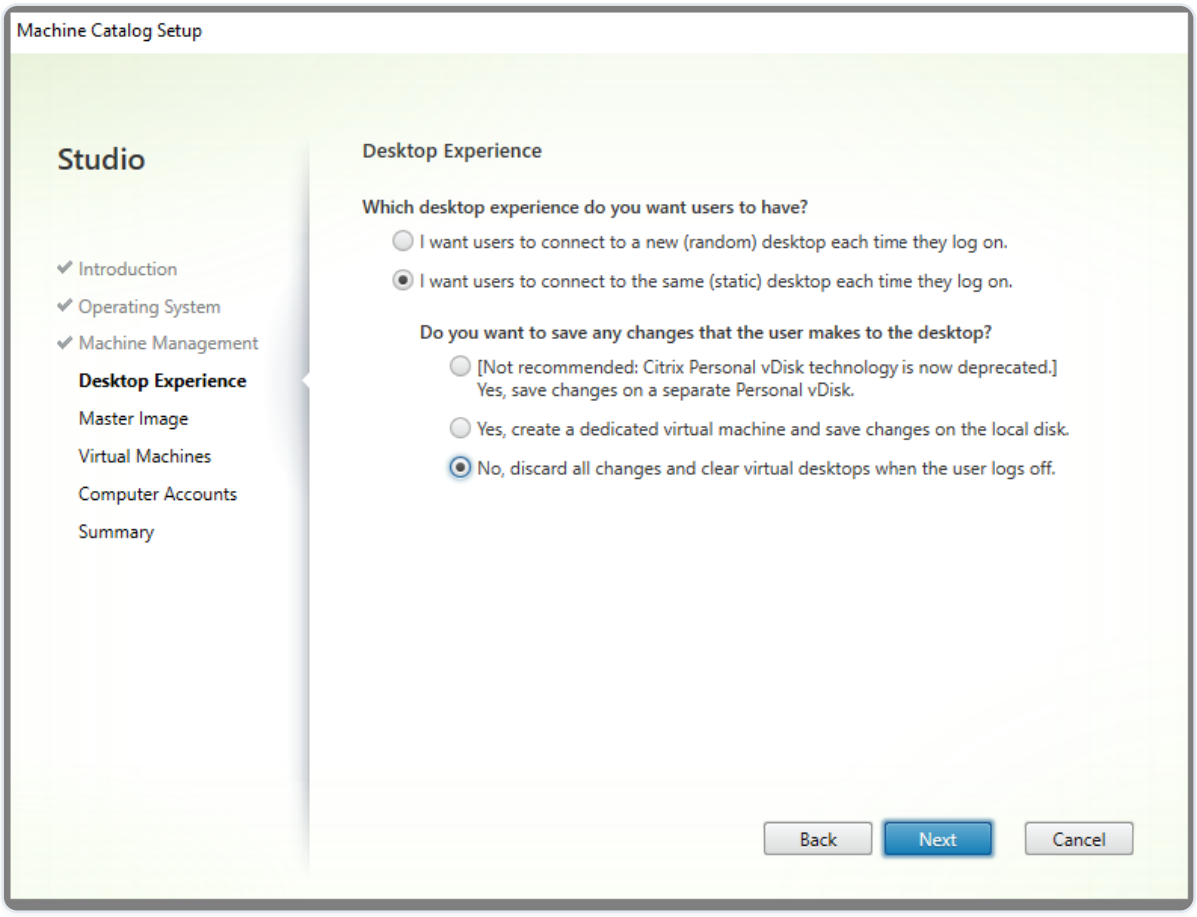
No Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

1. Selecione **Sistema Operacional** e defina-o como **SO de sessão única**.
2. Selecione **Gerenciamento de Máquinas** e defina-o como **Máquinas com gerenciamento de energia**. Por exemplo, máquinas virtuais ou PCs blade.
3. Selecione **Experiência de Área de Trabalho** e defina-o como tipo de catálogo **pooled-random** ou **pooled-static**, como nos exemplos a seguir:

   - **Pooled-random:**



- **Estático agrupado:** Se você selecionar estático agrupado, 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 captura de tela a seguir:



> **Nota:**
>
> A camada de personalização do usuário não oferece suporte a catálogos estáticos agrupados configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se você estiver usando o MCS, selecione **Imagem Mestra** e o instantâneo da 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.

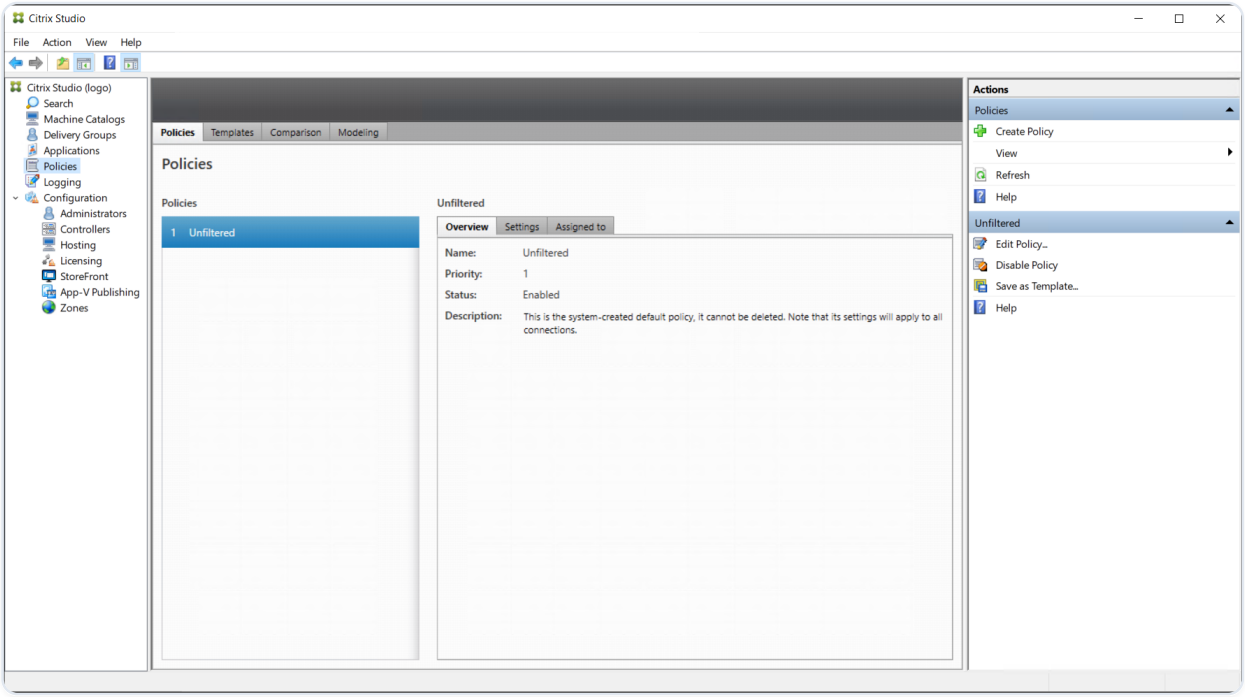
Etapa 5: Criar políticas personalizadas de grupo de entrega

Para habilitar a montagem de camadas de usuário dentro dos Agentes de Entrega Virtual, você usa os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- Qual o tamanho máximo permitido para o crescimento dos discos da camada de usuário.

Para definir os parâmetros como políticas personalizadas do Citrix no Studio e atribuí-los ao seu grupo de entrega.

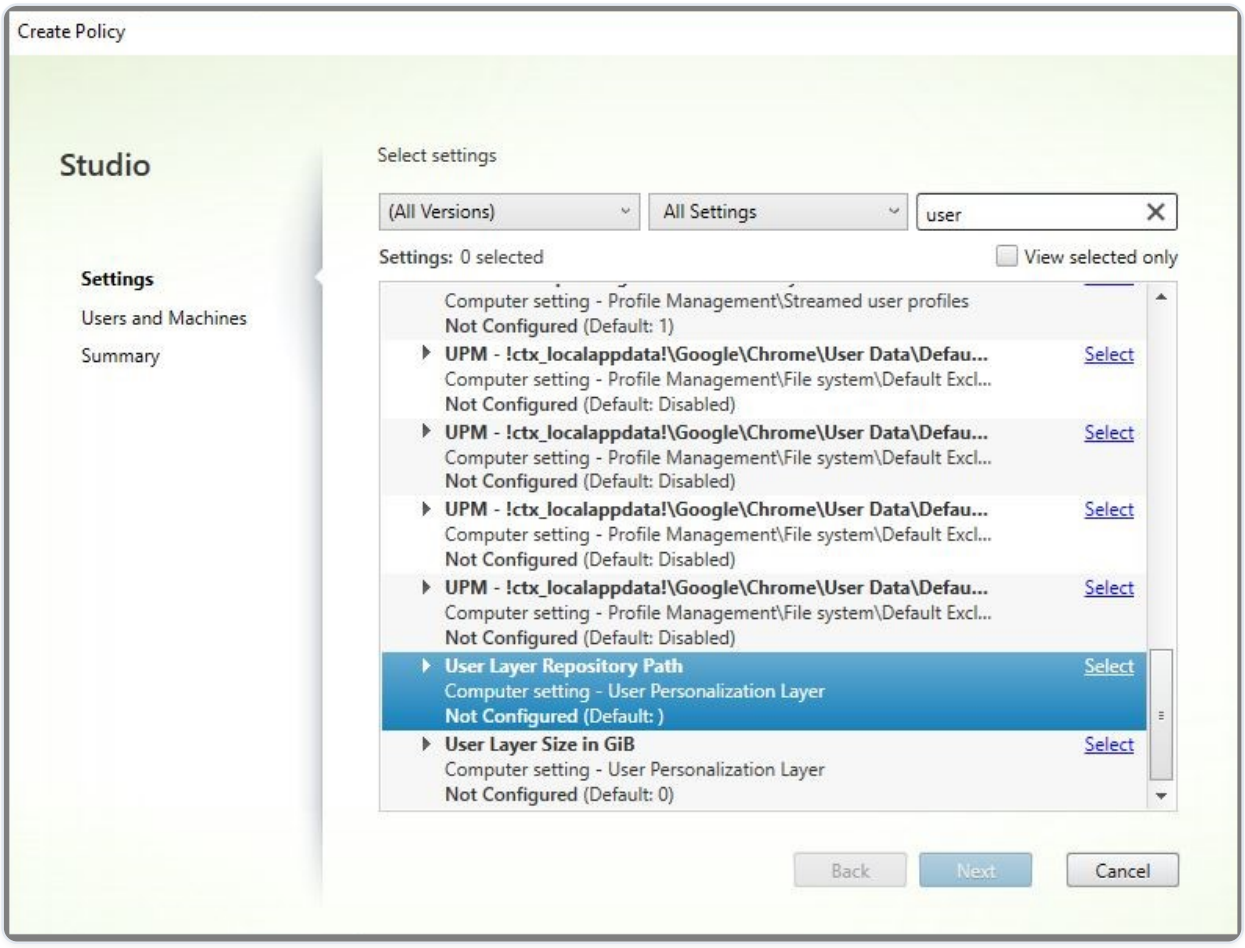
1. No Studio, selecione Políticas no painel de navegação:



2. Selecione Criar Política no painel Ações. A janela Criar Política é exibida.
3. Digite ‘camada de usuário’ no campo de pesquisa. As duas políticas a seguir aparecem na lista de políticas disponíveis:
    - Caminho do Repositório da Camada de Usuário
    - Tamanho da Camada de Usuário GB

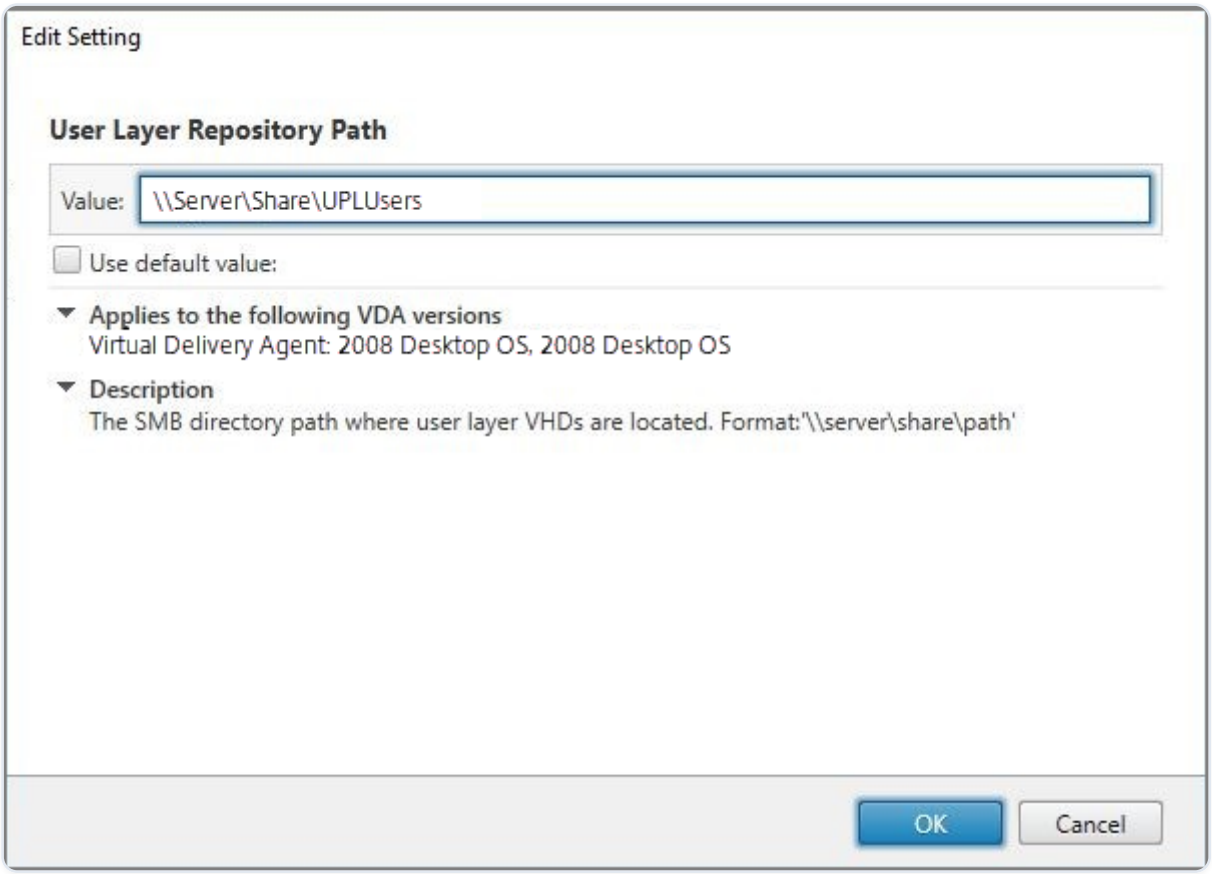
    > **Nota:**
    >
    > Aumentar o tamanho afeta novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

4. Clique em **Selecionar** ao lado de Caminho do Repositório da Camada de Usuário. A janela Editar Configuração é exibida.



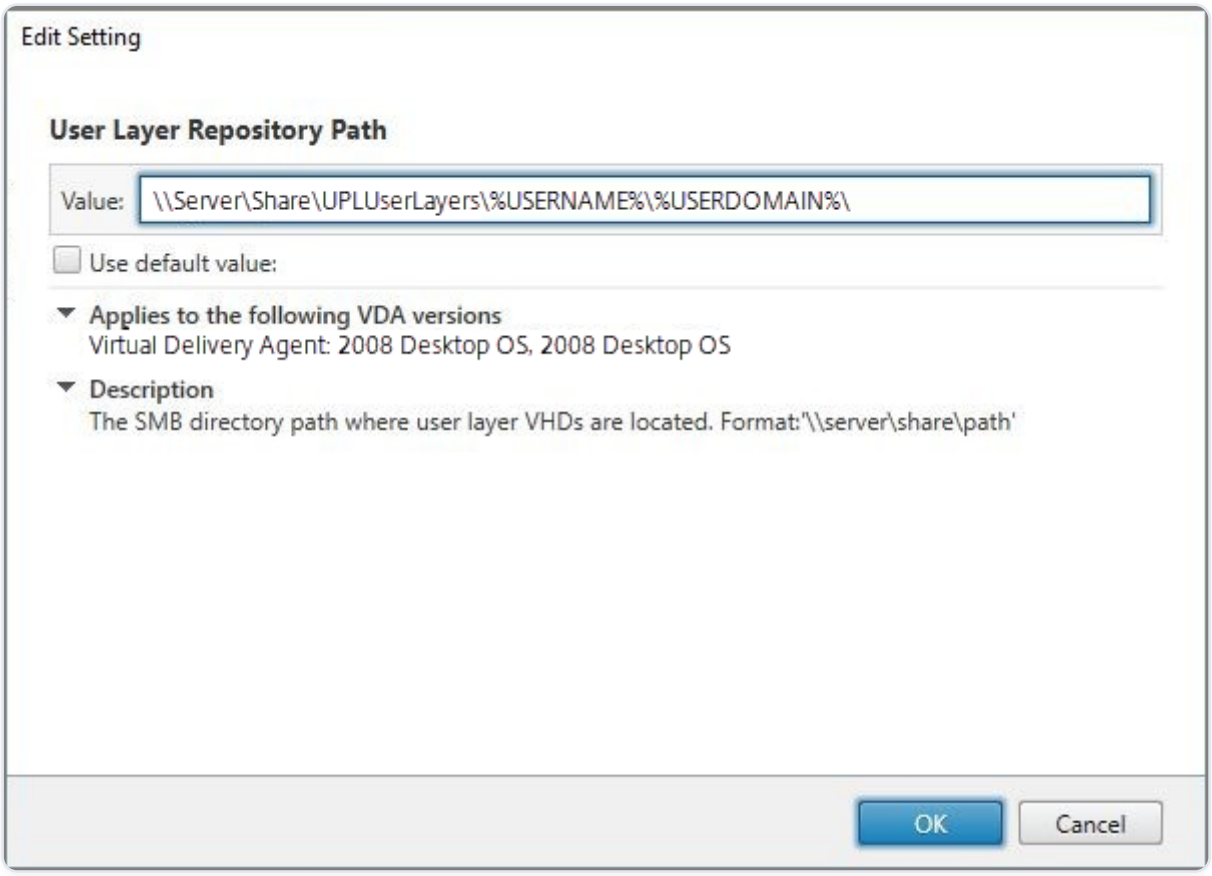
5. Insira um caminho no campo Valor e clique em **OK**:

   - **Formato do caminho:** `\\server-name-or-address\share-name\folder`
   - **Exemplo de caminho:** `\\Server\Share\UPLUsers`
   - **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

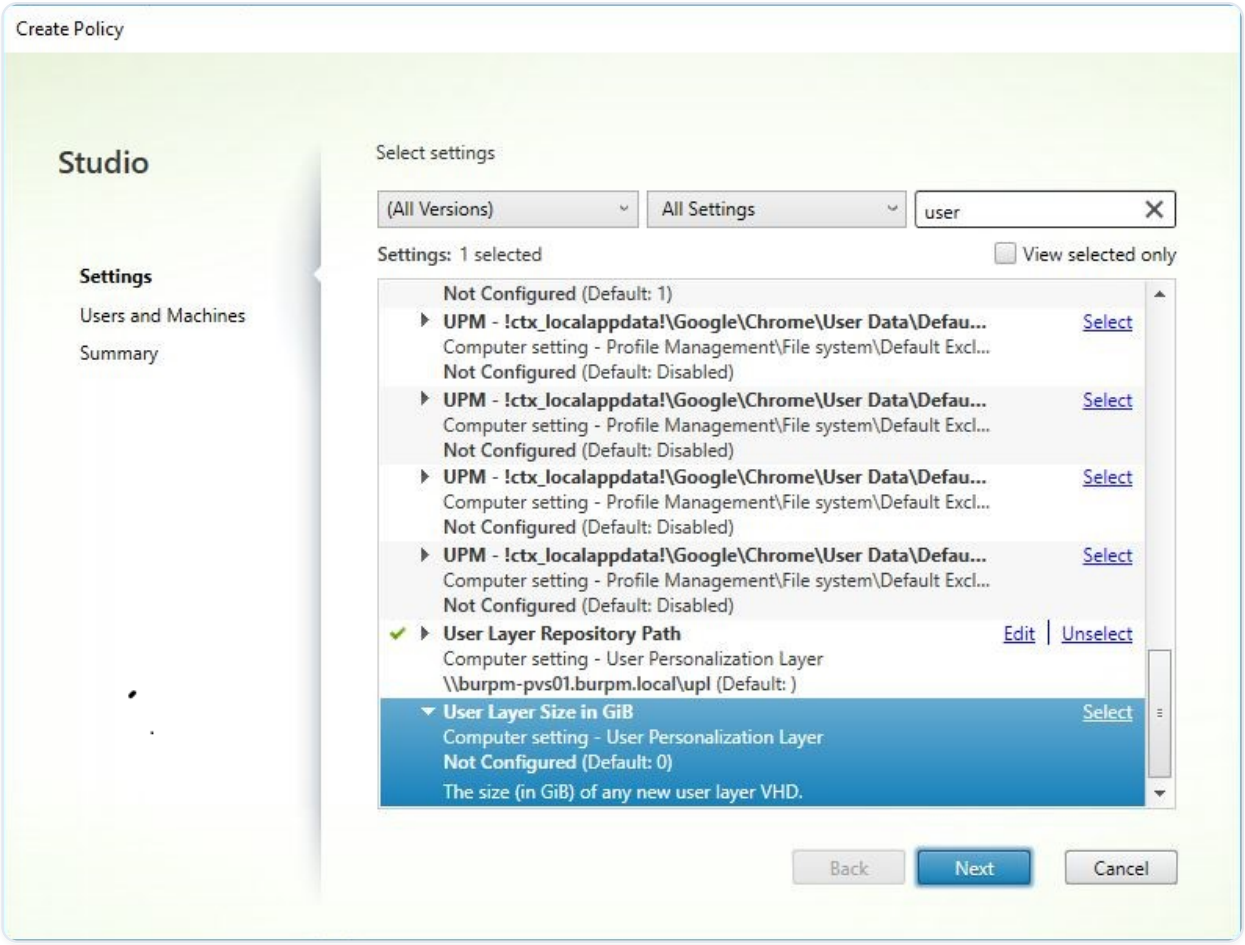


Você pode personalizar o caminho usando as variáveis, `%USERNAME%`, `%USERDOMAIN%`, e também variáveis de ambiente da máquina. Quando expandidas, essas variáveis resultam em caminhos explícitos.

- **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`

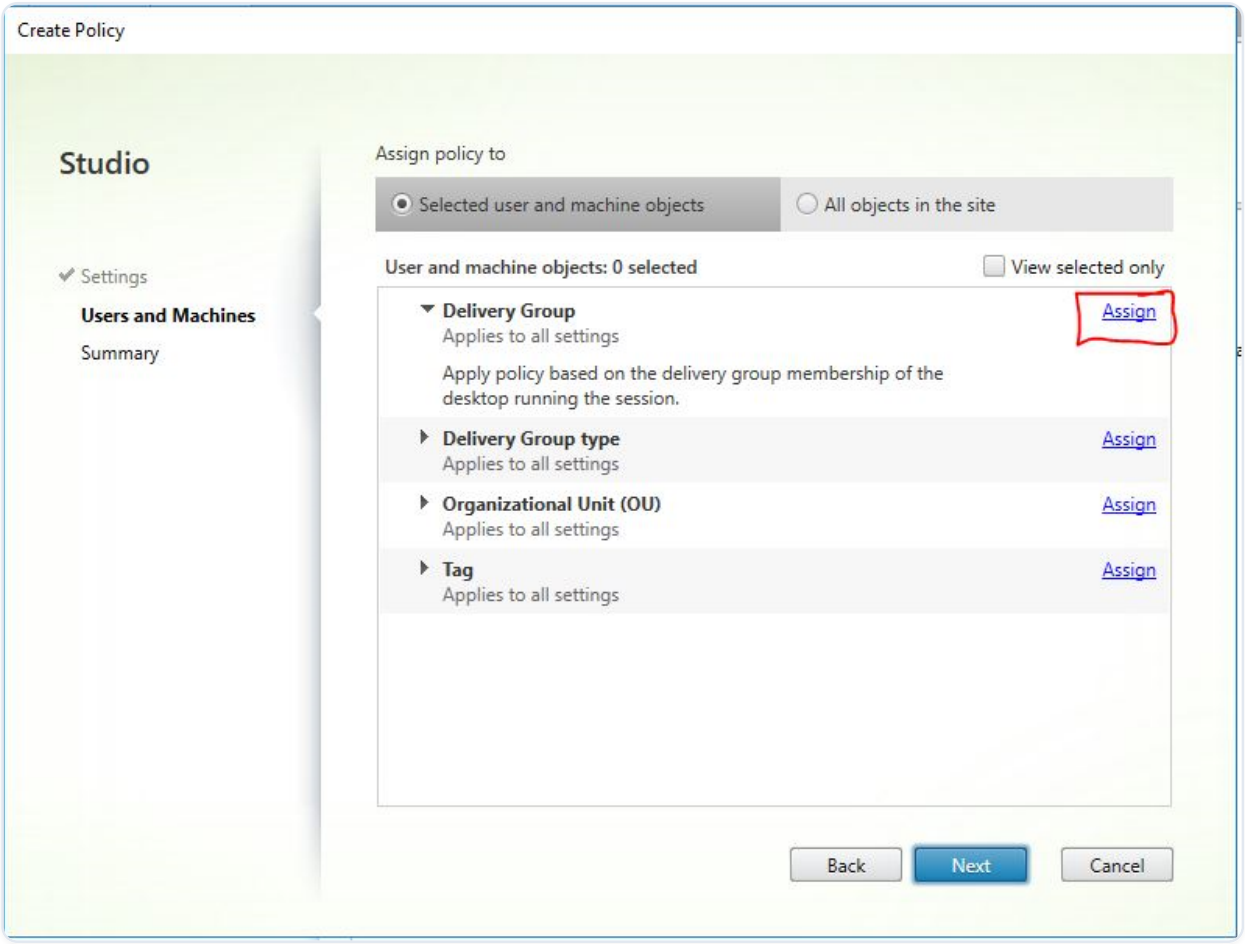


6. Opcional: Clique em **Selecionar** ao lado de Tamanho da Camada de Usuário em GB:

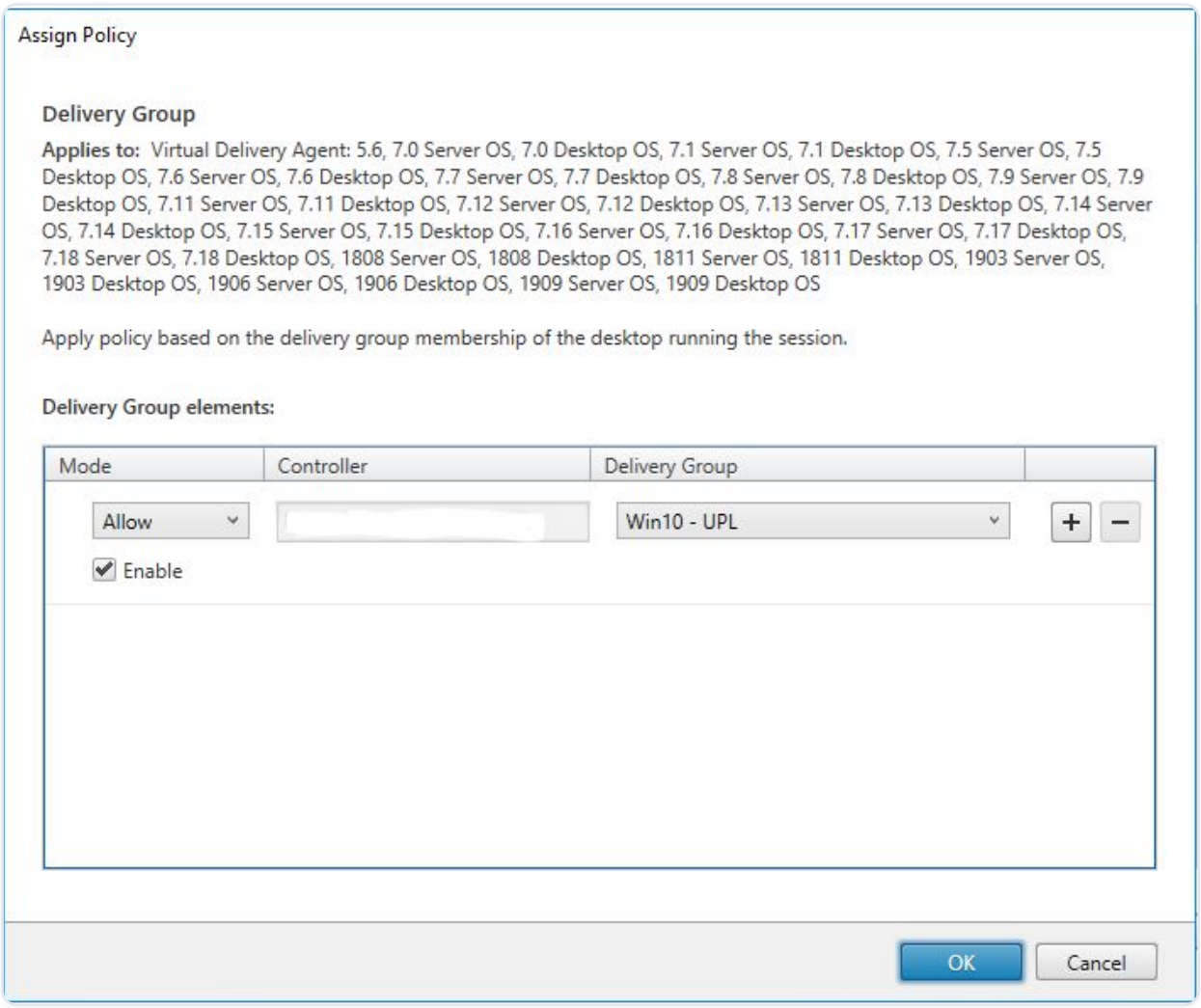


A janela Editar Configurações é exibida.

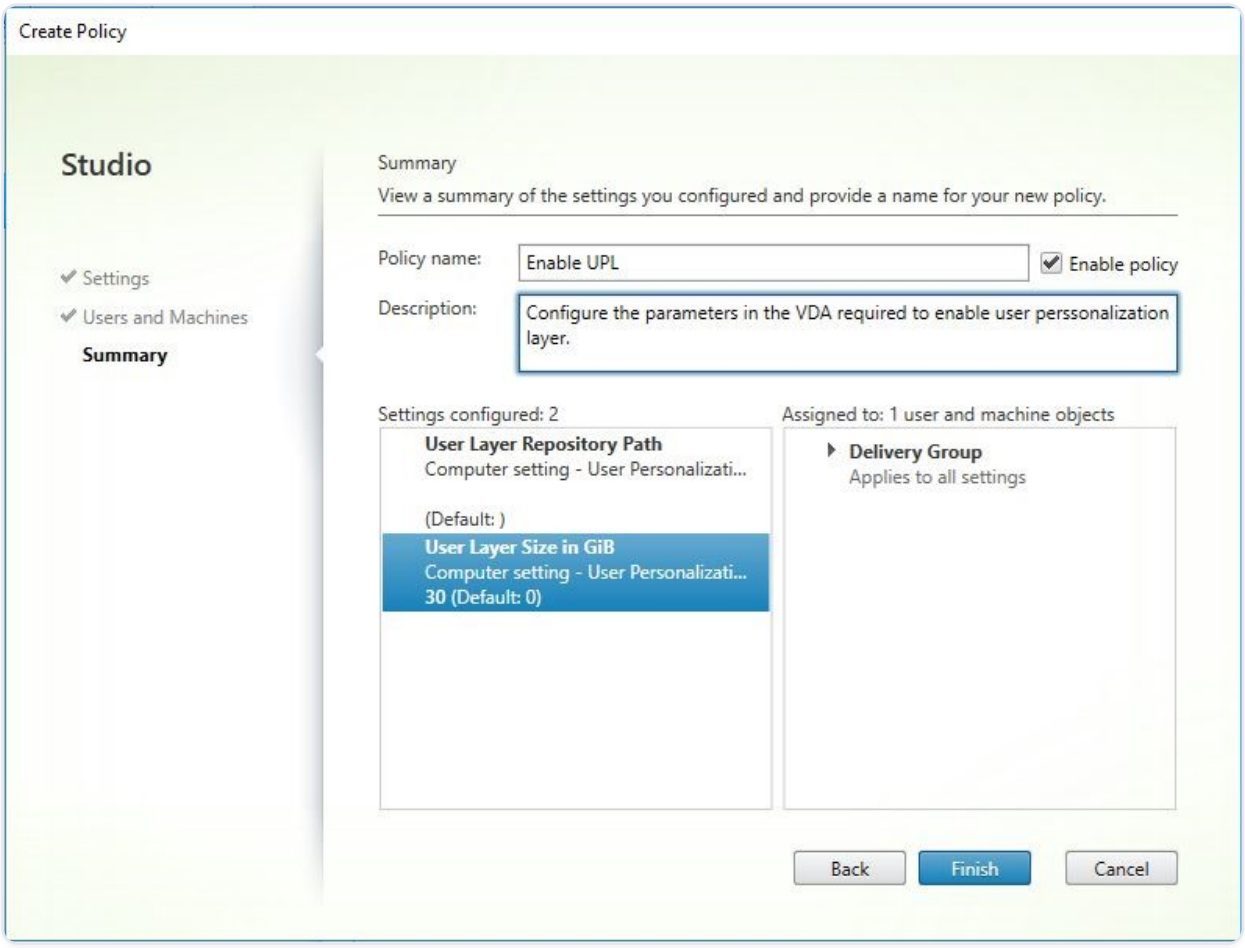
7. Opcional: Altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode atingir. Clique em **OK**.
8. Clique em **Avançar** para configurar Usuários e Máquinas. Clique no link Atribuir Grupo de Entrega destacado nesta imagem:



9. No menu Grupo de Entrega, selecione o grupo de entrega criado na seção anterior. Clique em OK.



10. 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; Percorrer Pasta/Executar Arquivo; Listar Pasta/Ler Dados; Ler Atributos	Somente Pasta Selecionada	

NOME DA CONFIGURAÇÃO	VALOR	APLICAR A	
Sistema	Controle Total	Pasta, Subpastas e Arquivos Selecionados	
Administradores de Domínio e grupo de Administradores selecionado	Controle Total	Pasta, Subpastas e Arquivos Selecionados	

Mensagens da camada de usuário

Quando um usuário não consegue acessar sua camada de usuário, ele recebe uma destas mensagens de notificação.

- **Camada de Usuário em Uso**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Camada de Usuário Indisponível**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Sistema não redefinido após o logoff do usuário**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

Arquivos de log para usar na solução de problemas

O arquivo de log, ulayersvc.log, contém a saída do software da camada de personalização do usuário, onde as alterações são registradas.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

Limitações

Tenha as seguintes limitações em mente ao instalar e usar o recurso de camada de personalização do usuário.

- *Não* tente implantar o software da camada de personalização do usuário em uma camada dentro do App Layering. Implante camadas de personalização do usuário no Citrix Virtual Apps and Desktops, ou habilite camadas de usuário em um modelo de imagem do App Layering, não ambos. Qualquer um dos processos produz as camadas de usuário de que você precisa.
- *Não* configure o recurso de camada de personalização do usuário com catálogos de máquinas persistentes.
- *Não* use hosts de sessão.
- *Não* atualize o catálogo de máquinas com uma imagem executando uma nova instalação do SO (mesmo que seja a mesma versão do Windows 10). A melhor prática é aplicar atualizações ao SO dentro da mesma imagem mestre usada ao criar o catálogo de máquinas.
- *Não* use drivers de tempo de inicialização, nem qualquer outra personalização de inicialização antecipada.
- *Não* migre dados PvD para o recurso de camada de personalização do usuário.
- *Não* migre camadas de usuário existentes do produto App Layering completo para o recurso de camada de personalização do usuário.
- *Não* altere o caminho SMB da camada de usuário para acessar camadas de usuário criadas usando uma imagem de SO mestre diferente.
- Quando um usuário faz logoff de uma sessão e depois faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Microsoft Software Center lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Indisponível** na segunda máquina.

  Para descobrir o status real do aplicativo, instrua o usuário a selecionar o aplicativo no Software Center e clicar em **Instalar**. O SCCM então atualiza o status para o valor 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 Implementar 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 a cada logon do usuário:

```
gpudate /Target:Computer /force
```

Para obter melhores resultados, aplique as alterações nas Configurações do Computador diretamente na camada do usuário, depois que o usuário tiver feito login.

- Uma conta de usuário de domínio não deve ser o último usuário a ter feito login em uma imagem mestre. Caso contrário, as máquinas provisionadas a partir dessa imagem terão problemas.

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 a Web Interface, você deve remover o componente Web Interface separadamente. Você não pode usar o instalador para remover a 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 comando a seguir remove o Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

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 é reiniciada 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

Observação:

O sistema de licenciamento baseado em arquivo, tradicionalmente usado para ativar vários componentes locais, terá seu 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 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 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.

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** tanto da sua Atualização Cumulativa (CU) atual quanto do seu LTSR de

destino (ou sua CU subsequente). Se a data de lançamento do seu ambiente atual for **posterior** à data de lançamento do LTSR de destino ou da CU do LTSR, a Citrix recomenda fortemente aguardar a próxima CU do LTSR mais recente. Proceder de outra forma pode fazer com que um código mais antigo sobrescreva atualizações de segurança existentes, patches de estabilidade e aprimoramentos 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**. Essa configuração específica pode resultar em um status de **'Sucesso Parcial'**.

Introdução

A atualização muda sua implantação para o Citrix Virtual Apps and Desktops 7 Versão Atual (CR) sem a necessidade de configurar novas máquinas ou sites. A atualização é conhecida 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 (/pt-br/citrix-virtual-apps-desktops/2203-ltsr/upgrade-migrate/upgrade.html) antes de iniciar a atualização. O artigo é a principal fonte de informação para aprender como se preparar e implementar uma atualização.
2. Conclua as orientações de preparação.
3. Execute os instaladores para atualizar os componentes principais.
4. Atualize os bancos de dados do sistema e o site.
5. Atualize os VDAs em imagens (ou diretamente nas máquinas).
6. 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™ 2203 LTSR a partir de:

- XenApp and XenDesktop 7.15 LTSR CU5 até o CU mais recente
- Virtual Apps and Desktops 1912 com ou sem CUs, até e incluindo o CU mais recente
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

O suporte à versão Current Release do Citrix Virtual Apps and Desktops está disponível em Atualizar uma implantação.

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 do 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 no site durante a mesma janela de manutenção?**

  A melhor prática é atualizar todos os Delivery Controllers durante a mesma janela de manutenção, pois vários serviços em cada Controller se comunicam entre si. Manter versões diferentes pode causar problemas. Durante uma janela de manutenção, recomendamos que você atualize metade dos Controllers, atualize o site e, em seguida, atualize os Controllers restantes. (Para obter detalhes, consulte o Procedimento de atualização.)

- **Posso ir diretamente para a versão mais recente ou preciso fazer atualizações incrementais?**

  Quase sempre é possível atualizar para a versão mais recente e pular versões intermediárias, a menos que explicitamente declarado no artigo **Novidades** da versão para a qual você está atualizando. Consulte o Guia de atualização.

- **Um cliente pode atualizar de um ambiente Long Term Service Release (LTSR) para um Current Release?**

  Sim. Os clientes não são obrigados a permanecer em uma Long Term Service Release por um período prolongado. Os clientes podem mover um ambiente LTSR para 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. Para obter mais informações, consulte Ciclo de vida do Current Release.

- **O que é recomendado: atualizar para LTSR ou CR?**

  Os Current Releases (CRs) oferecem os recursos e funcionalidades mais recentes e inovadores de virtualização de aplicativos, desktops e servidores. Isso permite que você se mantenha na vanguarda da tecnologia e à frente da concorrência.

  Os Long Term Service Releases (LTSRs) são ideais para grandes ambientes de produção corporativos que preferem manter a mesma versão base por um período prolongado.

  Para obter detalhes, consulte Opções de serviço.

- **Preciso atualizar minhas licenças?**

  Certifique-se de que a data da licença atual não expirou e é válida para a versão para a qual você está atualizando. Consulte CTX111618. Para obter informações sobre renovação, consulte licenças de renovação dos Serviços de Sucesso do Cliente.

- **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 atinge o EOL?**

  Verifique a Matriz de Produtos.

- **Quais são os problemas conhecidos com a versão mais recente?**

  - Aplicativos e Desktops Virtuais Citrix
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - Citrix Workspace app para Windows

Mais informações

Long Term Service Release (LTSR) as atualizações de implantação usam Atualizações Cumulativas (CUs). Uma CU atualiza os componentes de linha de base do LTSR, e cada CU inclui seu próprio metainstalador.

Cada CU tem documentação dedicada. Por exemplo, para o LTSR 7.15, verifique o link na página **Novidades** desse LTSR para a CU mais recente. Cada página da CU inclui informações de versão suportadas, instruções e um link para o pacote de download da CU.

Migrar

Migrar para a nuvem

Você pode usar a ferramenta de Configuração Automatizada para Citrix Virtual Apps and Desktops para migrar sua implantação local para a nuvem. Para 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.

Para conteúdo de migração anterior 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 **Alterações na versão 7.x**, **Atualizar um worker do XenApp 6.5 para um novo VDA** e **Migrar XenApp 6.x**, consulte o arquivo legado do Citrix Virtual Apps and Desktops em `<https://docs.citrix.com/pt-br/legacy-archive/citrix-virtual-apps-and-desktops.html>`.

Atualizar uma implantação

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. License Activation Service (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 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

Você pode atualizar certas implantações para versões mais recentes sem precisar configurar novas máquinas ou sites primeiro. Isso é chamado de atualização in-place.

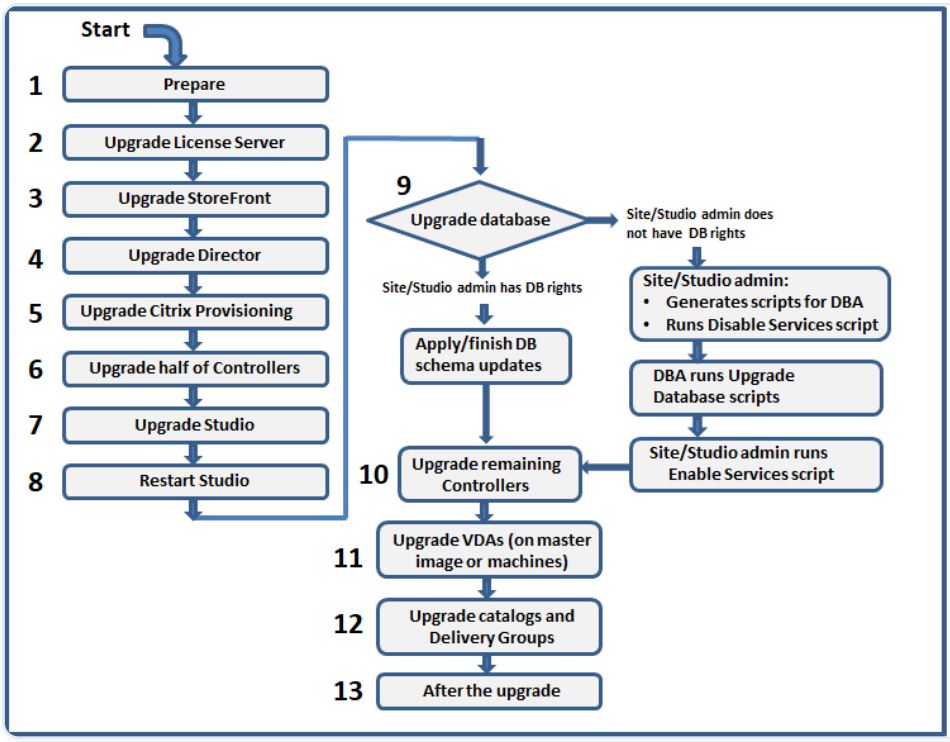
Para iniciar uma atualização, você executa o instalador da nova versão para atualizar os componentes principais, VDAs e outros componentes previamente instalados. Em seguida, você atualiza os bancos de dados e o site.

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.



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 prazo 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 fazer upgrade 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 upgrades e criação de sites.

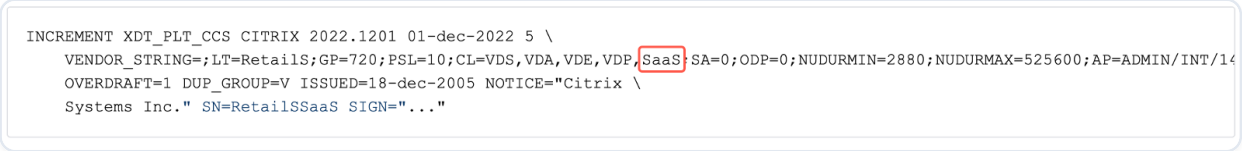
Se você fizer upgrade do Citrix Virtual Apps and Desktops LTSR 1912 para o LTSR 2203 e tiver direito a novas licenças de Direitos Híbridos com uma conexão Azure, AWS ou Google Cloud, certifique-se de seguir estas etapas. Caso contrário, seu meta instalador 2203 bloqueará seu upgrade:

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. Vá para 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 Incrementos.



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 o upgrade in-place. 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 upgrade

A maioria dos principais componentes do produto pode ser atualizada executando o instalador do produto na máquina que contém o componente.

Se uma máquina contiver mais de um componente (por exemplo, Studio e License Server), todos os componentes dessa máquina serão atualizados, se a mídia do produto contiver versões mais recentes de seu 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 o seu License Server é compatível com a nova versão, é essencial que você execute o instalador no License Server antes de atualizar quaisquer outros componentes principais.

Etapa 3: Atualizar o StoreFront™

Se a mídia de instalação contiver uma nova versão do software StoreFront, execute o instalador na máquina que contém o servidor StoreFront.

- Na interface gráfica, escolha **Citrix StoreFront** na seção **Estender implantação**.
- Na linha de comando, execute `CitrixStoreFront-x64.exe`, que está disponível na pasta `x64` da mídia de instalação do Citrix Virtual Apps and Desktops.

Etapa 4: Atualizar o Director

Se a mídia de instalação contiver uma nova versão do software Director, execute o instalador na máquina que contém o Director.

Etapa 5: Atualizar o Citrix Provisioning

A mídia de instalação do Citrix Provisioning está disponível separadamente da mídia de instalação do Citrix Virtual Apps and Desktops. Para saber como instalar e atualizar o servidor Citrix Provisioning e o software do dispositivo de destino, consulte a documentação do produto Citrix Provisioning.

Etapa 6: Atualizar metade dos Delivery Controllers

Por exemplo, se o seu site tiver quatro Controllers, execute o instalador em dois deles.

Deixar metade dos Controllers ativos permite que os usuários acessem o site. Os VDAs podem se registrar nos Controllers restantes. Pode haver momentos em que o site tenha capacidade reduzida porque menos Controllers estão disponíveis. A atualização causa apenas uma breve interrupção no estabelecimento de novas conexões de cliente durante as etapas finais de atualização do banco de dados. Os Controllers atualizados não podem processar solicitações até que todo o site seja atualizado.

Se o seu site tiver apenas um Controller, ele ficará inoperável durante a atualização.

Testes preliminares do site são executados no primeiro Controller, antes do início da atualização real. Para obter detalhes, consulte Testes preliminares do site.

Etapa 7: Atualizar o Studio

Se você ainda não atualizou o Studio (porque ele estava na mesma máquina que outro componente), execute o instalador na máquina que contém o Studio.

Etapa 8: Reiniciar o Studio

Reinicie o Studio atualizado. O processo de atualização é retomado automaticamente.

Etapa 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 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.

> Verifique Preparação para as permissões necessárias para atualizar o esquema dos bancos de dados do SQL Server.

- Se você tiver permissão suficiente para atualizar o esquema do banco de dados do SQL Server, poderá iniciar uma atualização automática do banco de dados. Continue com Atualizar o banco de dados e o site automaticamente.
- Se você não tiver permissões de banco de dados suficientes, poderá iniciar uma atualização manual que usa scripts e prosseguir com a ajuda do seu administrador de banco de dados (alguém que tenha as permissões necessárias). Para uma atualização manual, o usuário do

Studio gera os scripts e, em seguida, executa os scripts que habilitam e desabilitam os serviços. O administrador do banco de dados executa outros scripts que atualizam o esquema do banco de dados, usando o utilitário SQLCMD ou o SQL Server Management Studio no modo SQLCMD. Continue com Atualizar o banco de dados e o site manualmente.

- Se você tiver uma implantação multizona e quiser atualizar o banco de dados e o site automaticamente, a Citrix recomenda que a atualização do dbschema seja realizada na mesma zona que hospeda os bancos de dados do SQL Server do site. Caso contrário, a atualização automática do banco de dados e do site poderá falhar.

A Citrix recomenda fortemente que você faça backup do banco de dados antes de atualizar. Consulte CTX135207. Durante uma atualização 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 se você fez backup do banco de dados.

   O assistente gera e exibe os scripts e uma lista de verificação das etapas de atualização. Se o esquema de um banco de dados não foi alterado desde a versão do produto que está sendo atualizada, esse script não é gerado. Por exemplo, se o esquema do banco de dados de log não for alterado, o script `UpgradeLoggingDatabase.sql` não será gerado.
4. Execute os seguintes scripts na ordem mostrada.

   - `DisableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para desabilitar os serviços do produto.
   - `UpgradeSiteDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Site

- `UpgradeMonitorDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Monitor.
- `UpgradeLoggingDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados de Log de Configuração. Execute este script somente se este banco de dados for alterado (por exemplo, após aplicar um hotfix).
- `EnableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para habilitar os serviços do produto.

Após a conclusão da atualização do banco de dados e a habilitação dos serviços do produto, o Studio testa automaticamente o ambiente e a configuração e, em seguida, gera um relatório HTML. Se problemas forem identificados, você poderá restaurar o backup do banco de dados. Após resolver os problemas, você pode atualizar o banco de dados novamente.

5. Após concluir as tarefas da lista de verificação, clique em **Concluir atualização**.

Etapa 10: Atualizar os Delivery Controllers restantes

No Studio recém-atualizado, selecione **Citrix Studio** *nome-do-site* no painel de navegação. Na guia **Tarefas Comuns**, selecione **Atualizar os Delivery Controllers restantes**.

Após concluir a atualização e confirmar a conclusão, feche e reabra o Studio. O Studio pode solicitar uma atualização extra do site para registrar os serviços do Controller no site ou para criar um ID de zona, se ele não existir.

Etapa 11: Atualizar VDAs

> **Importante:**

> Se você estiver atualizando um VDA para a versão 1912 ou posterior, consulte Atualizando VDAs para 1912 ou posterior.

> Execute o instalador do produto nas máquinas que contêm VDAs.

Se você usou o Machine Creation Services™ e uma imagem mestre para criar máquinas, vá para o seu host e atualize o VDA na imagem mestre. Você pode usar qualquer um dos instaladores de VDA disponíveis.

- Para obter orientação sobre a interface gráfica, consulte Instalar VDAs.
- Para obter orientação sobre a linha de comando, consulte Instalar usando a linha de comando.

Se você usou o Citrix Provisioning para criar máquinas, consulte a documentação do produto Citrix Provisioning para obter orientação sobre a atualização.

Etapa 12: Atualizar catálogos de máquinas e grupos de entrega

- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar grupos de entrega que usam máquinas com VDAs atualizados.

Etapa 13: Após a atualização

Após concluir uma atualização, você pode testar o site recém-atualizado. No Studio, selecione **Citrix Studio site-name** no painel de navegação. Na guia **Common Tasks**, selecione **Test Site**. Esses testes são executados automaticamente após a atualização do banco de dados, mas você pode executá-los novamente a qualquer momento.

Os testes podem falhar para um Controller no Windows Server 2016 quando um Microsoft SQL Server Express local é usado para o banco de dados do site, se o Serviço de Navegador do SQL Server não estiver iniciado. Para evitar isso:

- Habilite o Serviço de Navegador do SQL Server (se necessário) e, em seguida, inicie-o.
- Reinicie o serviço SQL Server (SQLEXPRESS).

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 RTM	2203 CU1	2203 CU2	2203 CU3
7.15 RTM/CU	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU1		Site	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU2			Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU3				Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU4					Site; Config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU5						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU6						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU7						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
2203 RTM							Config	Config	Config
2203 CU1								Config	Config
2203 CU2									Config

Definição dos termos:

- Site: 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.
- Logging: Datastore de Log. A atualização do Dbschema é feita no Datastore de Log.

Atualizar VDAs para 2203 ou posterior

Se o componente Personal vDisk (PvD) foi instalado em um VDA, esse VDA não pode ser atualizado para a versão 2203 ou posterior. Para usar o novo VDA, você deve desinstalar o VDA atual e, em seguida, instalar o novo VDA.

Esta instrução se aplica mesmo que você nunca tenha usado o PvD.

Veja como o componente PvD pode ter sido instalado em versões anteriores:

- Na interface gráfica do instalador do VDA, o PvD era uma opção na página **Componentes Adicionais**. As versões 7.15 LTSR e 7.x anteriores habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou habilitou explicitamente a opção em qualquer versão), o PvD foi instalado.
- Na linha de comando, a opção `/baseimage` instalava o PvD. Se você especificou essa opção, ou usou um script que continha essa opção, o PvD foi instalado.

Se você não sabe se o seu VDA tem o PvD instalado, execute o instalador do novo VDA (2203 ou posterior) na máquina ou 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 o PvD instalado:

1. Desinstale o VDA atual.
2. Instale o novo VDA.

Se você quiser continuar usando o PvD em suas máquinas Windows 10 (1607 e anteriores, sem atualizações), o VDA 7.15 LTSR é a versão mais recente suportada.

> **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 existentes de PvD no Windows 7 a migrar para a tecnologia Citrix App Layering, a Citrix decidiu fornecer suporte por tempo limitado para implantações de PvD para desktops Windows 7 por meio das Atualizações Cumulativas (CUs) do XenApp e XenDesktop 7.15 LTSR até Jan 14, 2020. O componente PvD será removido das CUs do LTSR e não será suportado após Jan 14, 2020. Além disso, o uso de PvD para Windows 7 após Jan 14, 2020 tornará os sites LTSR não conformes. Além disso, o PvD para Windows 10 continua sendo excluído do 7.15 LTSR. Portanto, os clientes não devem usá-lo com seus sites 7.15 LTSR.

Remover PvD, AppDisks e hosts não suportados

As seguintes tecnologias e tipos de host não são suportados em implantações do Citrix Virtual Apps and Desktops 7 Current Release:

- **Personal vDisks (PvD)** para armazenar dados próximos às VMs dos usuários em catálogos. O recurso de camada de personalização do usuário agora lida com a persistência do usuário.
- **AppDisks** para gerenciar aplicativos usados em Delivery Groups.
- **Tipos de host:** Azure Classic, CloudPlatform (o produto Citrix original).
    - Para os 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 posteriores suportadas) 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
- Remover AppDisks
- Remover itens de host não suportados

Mesmo que você não tenha usado PvD ou AppDisks em sua implantação, MSIs relacionados podem ter sido incluídos em uma instalação ou atualização anterior do VDA. Antes de poder atualizar seus VDAs para a versão 2006 (ou uma versão posterior suportada), 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, em seguida, remova os próprios AppDisks.

1. Selecione **Delivery Groups** no painel de navegação do Studio.
2. Selecione um grupo e clique em **Gerenciar AppDisks** no painel Ação.
3. Clique na ação que remove o AppDisk do grupo.
4. Repita os passos 2 e 3 para cada Delivery Group que usa AppDisks.
5. Selecione **AppDisks** no painel de navegação do Studio.
6. Selecione um AppDisk e clique na ação que exclui o AppDisk.
7. Repita as etapas 5 e 6 para cada AppDisk.

Atualizações de VDA: A atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores do VDA detectam. Para obter detalhes, consulte VDAs que têm componentes PvD ou AppDisks.

Remover itens de host não suportados

Uma atualização de implantação para a versão 2006 (ou versão posterior suportada) 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 Delivery Group 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, você é perguntado se 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 anteriores 7.x habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou habilitou explicitamente a opção em qualquer versão que a oferecesse), esse componente foi instalado.
- CLI: A especificação da opção `/baseimage` instalou o componente.

O que fazer

Se o instalador do VDA não detectar os componentes AppDisks ou PvD no VDA atualmente instalado, a atualização prosseguirá normalmente.

Se o instalador detectar componentes AppDisks ou PvD no VDA atualmente instalado:

- Interface gráfica: A atualização é pausada. Uma mensagem pergunta se você deseja que os componentes não suportados sejam removidos automaticamente. Se você clicar em **OK**, os componentes são removidos automaticamente e a atualização prossegue.
- CLI: Para evitar falha no comando, inclua as seguintes opções no comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

Limitações

As seguintes limitações se aplicam às atualizações:

- **Instalação seletiva de componentes:** Se você instalar ou atualizar quaisquer componentes para a nova versão, mas optar por não atualizar outros componentes (em máquinas diferentes) que 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 Early Release ou Technology Preview:** Você não pode atualizar de uma versão Early Release, Technology Preview ou de pré-visualização.
- **Componentes em sistemas operacionais anteriores:** Você não pode instalar VDAs atuais em sistemas operacionais que não são mais suportados pela Microsoft ou Citrix. Para obter mais informações, consulte Sistemas operacionais anteriores.
- **Ambientes/sites mistos:** Se você precisar continuar a executar sites de versões anteriores e sites de versões atuais, consulte Considerações sobre ambientes mistos.
- **Seleção de produto:** Ao atualizar de uma versão anterior, você não escolhe ou especifica o produto (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) que foi definido durante a instalação.

Considerações sobre ambientes mistos

Ao atualizar, a Citrix recomenda que você atualize todos os componentes e VDAs para que possa acessar todos os recursos novos e aprimorados em sua edição e versão.

Por exemplo, embora você possa usar VDAs atuais em implantações contendo versões anteriores do Controller, novos recursos na versão atual podem não estar disponíveis. Problemas de registro de VDA também podem ocorrer ao usar versões não atuais.

Em alguns ambientes, talvez você não consiga atualizar todos os VDAs para a versão mais atual. Nesse caso, ao criar um catálogo de máquinas, você pode especificar a versão do VDA instalada nas máquinas. (Isso é chamado de nível funcional.) Por padrão, essa configuração especifica a versão mínima recomendada do VDA. O valor padrão é suficiente para a maioria das implantações. Considere alterar a configuração para uma versão anterior somente se o catálogo

contiver VDAs anteriores ao padrão. Não é recomendável misturar versões de VDA em um catálogo de máquinas.

Se um catálogo for criado com a configuração padrão de versão mínima do VDA, e uma ou mais máquinas tiverem um VDA anterior à versão padrão, essas máquinas não poderão se registrar no Controller e não funcionarão.

Para obter mais informações, consulte Versões de VDA e níveis funcionais.

Vários sites com versões diferentes

Quando seu ambiente contém sites com diferentes versões de produto (por exemplo, um site XenDesktop 7.18 e um site Citrix Virtual Apps and Desktops 1909), a Citrix recomenda usar o StoreFront para agregar aplicativos e desktops de diferentes versões de produto. Para obter detalhes, consulte a documentação do StoreFront.

Em um ambiente misto, continue usando as versões do Studio e do Director para cada lançamento, mas certifique-se de que versões diferentes 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 atualizar esse VDA para a versão atual, mas o Windows Server 2008 R2 não é compatível com a versão atual para a qual você está atualizando.

Se você tentar instalar ou atualizar um componente em um sistema operacional que não é mais permitido, uma mensagem de erro é exibida, como "Não pode ser instalado neste sistema operacional".

Essas considerações se aplicam à atualização das versões Current Release e Long Term Service Release. (Não afeta a aplicação de CUs a uma versão LTSR.)

Siga os links para saber quais sistemas operacionais são compatíveis:

- Citrix Virtual Apps and Desktops (Versão Atual):
  - Delivery Controller, Studio, Director, VDAs, Universal Print Server

  - Serviço de Autenticação Federada(/pt-br/federated-authentication-service/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 de componente válida mais recente suportada para cada SO listado e a versão do componente quando a instalação e a atualização se tornaram inválidas.

Os sistemas operacionais na tabela incluem service packs e atualizações.

SISTEMA OPERACIONAL	COMPONENTE/ RECURSO	VERSÃO VÁLIDA MAIS RECENTE	INSTALAÇÃO/ ATUALIZAÇÃO NÃO É POSSÍVEL A PARTIR DA VERSÃO
Windows 7 e Windows 8	VDA	7.15 LTSR	7.16
Windows 7 e Windows 8	Outros componentes do instalador	7.17	7.18
Versões do Windows 10 anteriores a 1607	VDA	7.15 LTSR	7.16
Versão x86 do Windows 10	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

SISTEMA OPERACIONAL	COMPONENTE/ RECURSO	VERSÃO VÁLIDA MAIS RECENTE	INSTALAÇÃO/ ATUALIZAÇÃO NÃO É POSSÍVEL A PARTIR DA VERSÃO
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	VDI de Servidor	7.15 LTSR	7.16

Windows XP e Windows Vista não são válidos para nenhum componente ou tecnologia 7.x.

* Aplica-se a Delivery Controller, Studio, Director e VDAs.

O que você pode fazer

Você tem opções. Você pode:

- Continuar com o SO atual
- Reimagear ou atualizar a máquina
- Adicionar novas máquinas e depois remover as antigas

Continuar com o sistema operacional atual

Esses métodos são viáveis para VDAs. Se você quiser continuar usando máquinas com o SO anterior, pode escolher uma das seguintes opções:

- Continuar usando a versão do componente instalada.
- Baixe a versão mais recente do componente válido e, em seguida, atualize o componente para essa versão. (Isso pressupõe que a versão mais recente do componente válido ainda não esteja instalada.)

Por exemplo, você tem um VDA 7.14 em uma máquina Windows 7 SP1. A 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 Citrix Virtual Apps and Desktops 7 1808.

Reimagear ou atualizar a máquina

Esses métodos são viáveis para VDAs e outras máquinas que não possuem componentes principais (como Delivery Controllers) instalados. Escolha uma das seguintes opções:

- Depois de desativar a máquina (ativando o modo de manutenção e permitindo que todas as sessões sejam encerradas), você pode reimaginá-la para uma versão de SO Windows compatível e, em seguida, instalar a versão mais recente do componente.
- Para atualizar o SO em uma máquina VDA sem reimagem, você deve primeiro instalar a versão do VDA compatível com o SO para o qual você está atualizando ou atualizar o VDA após a atualização do SO. Caso contrário, o software Citrix não será compatível. Você pode atualizar para as seguintes versões mínimas de SO ao realizar uma atualização in-loco sem desinstalar o VDA:
  - Windows 11 com Atualização Cumulativa de 2023-07 para Windows 11 (KB5028185) ou posterior instalado (compilação 22621.1992 ou posterior).
  - Windows 10 com Atualização Dinâmica de 2023-07 para Windows 10 (KB5028311) instalado.
- Se a versão do Windows para a qual você planeja atualizar não estiver alinhada com a diretriz mencionada, você deve desinstalar o VDA antes de atualizar o SO e, em seguida, instalar uma versão VDA compatível após a conclusão da atualização do SO.

Adicionar novas máquinas e, em seguida, remover máquinas antigas

Esse 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 sequência de atualização a seguir 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 informações a seguir e conclua as tarefas necessárias.

> **Nota:**
>
> 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 uma interface

Use o instalador completo do produto do ISO do produto para atualizar os componentes. Você pode atualizar VDAs usando o instalador completo do produto ou um dos instaladores de VDA autônomos. Todos os instaladores oferecem interfaces gráficas e de linha de comando.

Para obter mais informações, consulte Instaladores.

Detalhes da instalação: Depois de concluir qualquer trabalho de preparação e estar pronto para iniciar o instalador, o artigo de instalação mostra o que você verá (se estiver usando a interface gráfica) ou o que digitar (se estiver usando a interface de linha de comando).

- Instalar/atualizar componentes principais usando a interface gráfica
- Instalar/atualizar componentes principais usando a linha de comando
- Instalar/atualizar VDAs usando a interface gráfica
- Instalar/atualizar VDAs usando a linha de comando

Se você instalou originalmente um VDA de sessão única com o instalador `VDAWorkstationCoreSetup.exe`, a Citrix recomenda usar esse instalador para atualizá-lo. Se você usar o instalador VDA de produto completo ou o instalador `VDAWorkstationSetup.exe` para atualizar o VDA, os componentes que foram originalmente excluídos podem ser instalados, a menos que você os omita/exclua expressamente da atualização.

Ao atualizar um VDA para a versão atual, uma reinicialização da máquina ocorre durante o processo de atualização. (Este requisito começou com a versão 7.17.) Isso não pode ser evitado. A atualização é retomada automaticamente após a reinicialização (a menos que você especifique `/noresume` na linha de comando).

Ações do banco de dados

Faça backup dos bancos de dados de site, monitoramento e registro de configuração. Siga as instruções em CTX135207. Se algum problema for descoberto após a atualização, você poderá restaurar o backup.

Para obter informações sobre como atualizar versões do SQL Server que não são mais suportadas, consulte Verificação de versão do SQL Server. (Isso se refere ao SQL Server 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 quaisquer 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 Servidor de Licenças é compatível. Se o Servidor de Licenças 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.

Feche aplicativos e consoles

Antes de iniciar uma atualização, feche todos os programas que possam causar bloqueios de arquivos, incluindo consoles de administração e sessões do PowerShell.

Reiniciar a máquina garante que quaisquer bloqueios de arquivo sejam liberados e que não haja atualizações do Windows pendentes.

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 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

Quando você atualiza os Delivery Controllers e um site, testes preliminares do site são executados antes que a atualização real comece. Esses testes verificam:

- O banco de dados do site pode ser acessado e foi feito backup
- As conexões com os serviços essenciais da Citrix estão funcionando corretamente
- O endereço do Citrix License Server está disponível
- O banco de dados de log de configuração pode ser acessado
- Certifique-se de ter a Licença de Direitos Híbridos se quiser adicionar conexões de host de nuvem pública (por exemplo, AWS). Caso contrário, o teste preliminar do site pausa ou para, e uma mensagem explicativa aparece.

Após a execução dos testes, você pode visualizar um relatório dos resultados. 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 é sobrescrito.

Executar os testes

- Ao usar a interface gráfica do instalador para atualizar, o assistente inclui uma página onde você pode iniciar os testes e, em seguida, exibir o relatório. Após a execução dos testes e a visualização do relatório e a resolução de quaisquer problemas encontrados, você pode executar os testes novamente. Quando os testes forem concluídos com sucesso, clique em Avançar para continuar com o assistente.
- Ao usar a interface de linha de comando para atualizar, os testes são executados automaticamente. Por padrão, se um teste falhar, a atualização não 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 o upgrade 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 fazer upgrade de 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 do outro Controller.
- Se os testes no primeiro Controller estiverem em andamento ao iniciar a atualização no outro Controller, a página de testes do site aparecerá no assistente do outro Controller. No entanto, se os testes no primeiro Controller terminarem, somente 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 atualizando:
  - Interface gráfica: A atualização é interrompida com uma mensagem. Clique em **Entendi** e, em seguida, clique em **Cancelar** para fechar o instalador Citrix. (Você não pode continuar com a atualização.)
  - Interface de linha de comando: o comando falha (mesmo que você tenha incluído a opção `/ignore_db_check_failure` com o comando).

  Atualize a versão do SQL Server e, em seguida, inicie a atualização do Citrix novamente.
- Se a verificação não conseguir determinar qual versão do SQL Server está atualmente instalada, verifique se a sua versão atualmente instalada é compatível com a versão para a qual você está atualizando (Requisitos do sistema).
  - Interface gráfica: A atualização é interrompida com uma mensagem.
    - Se a versão do SQL Server atualmente instalada for compatível, clique em **Entendi** para fechar a mensagem e, em seguida, clique em **Avançar** para continuar com a atualização do Citrix.
    - Se a versão do SQL Server atualmente instalada não for compatível, 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 compatível 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 compatível, 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 Cache de Host Local usa de forma autônoma. O Cache de Host Local 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.

> **Observação:**

> O SQL Server Express LocalDB 2022 é suportado nas versões 2203 LTSR CU5 e posteriores do Citrix Virtual Apps and Desktops.

> 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 do Cache de Host Local que usa o 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 da 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 de Serviço de Rede. Você deve obter a seguinte saída: `nt authority\networkservice`.
7. Use o prompt de comando para navegar até a instância do SQL LocalDB:
   - Se estiver atualizando do SQL LocalDB 2014:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2017:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2019:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. 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 2019 como administrador no Delivery Controller.

    a. Use o arquivo `sqllocaldb.msi` na pasta `Support > SQLLocalDB` da mídia de instalação do Citrix Virtual Apps and Desktops. Por exemplo, se a mídia de instalação estiver montada na letra `E drive`, o arquivo pode ser encontrado em `E:\Support\SQLLocalDB\sqllocaldb.msi`. É necessário reiniciar para concluir a instalação.

    b. O novo SQL LocalDB deve estar em `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`.

15. Inicie o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
16. No Prompt de Comando do Delivery Controller, navegar para `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` e execute `SqlLocalDB i` para confirmar que a instância CitrixHA foi criada. O `CitrixHA` deve ser incluído na lista de instâncias retornadas.

> **Observação:**
>
> Pode levar até 15 minutos para que o banco de dados CitrixHA seja criado após o início do Serviço de Alta Disponibilidade do Citrix.

17. Certifique-se de que os arquivos de banco de dados do Cache de Host Local sejam criados para confirmar que o Serviço de Alta Disponibilidade (broker secundário) pode assumir o controle, se necessário.
    a. No Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
    b. Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.
18. Repita os passos nos Delivery Controllers restantes.

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 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 obter uma lista desses padrões, acesse `<https://www.commoncriteriaportal.org/cc/>`.

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 sua hora local ao usar desktops, consulte o artigo Gerenciar Grupos de Entrega.
- Um usuário que é administrador em um desktop tem controle total sobre esse desktop. Se um desktop for um desktop agrupado em vez de um desktop dedicado, o usuário deve ser confiável em relação a todos os outros usuários desse desktop, incluindo usuários futuros. Todos os usuários do desktop precisam estar cientes do risco potencial permanente à segurança de seus dados representado por essa situação. 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 que eles exigem. O direito de logon "Acessar este computador da rede" é necessário:

- Nos VDAs, para as contas de computador dos Delivery Controllers
- Nos 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 que eles exigem.

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 de múltiplas sessões 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 esta 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 provisionamento de AppDisks, integração AppDNA e gerenciamento de 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. Estes também são criados quando instalados com outros componentes Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Suporta a coleta de informações de diagnóstico para uso pelo Suporte Citrix.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Coleta informações de diagnóstico para análise pela Citrix, de modo que os resultados da análise e as recomendações possam ser visualizados pelos administradores para ajudar a diagnosticar problemas com o site.

A instalação do Delivery Controller também cria o seguinte serviço do Windows. Este não está sendo usado atualmente. Se tiver sido ativado, desative-o.

- Provider de Broker Remoto Citrix (NT SERVICE\XaXdCloudProxy)

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Eles 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 estão 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 Administrador Local no Delivery Controller. Isso permite que o Local Host Cache funcione corretamente.

O serviço de Administração Privilegiada do Citrix Storefront está configurado para fazer logon como Sistema Local (NT AUTHORITY\SYSTEM). Isso é necessário para operações do StoreFront do Delivery Controller que normalmente não estão disponíveis para serviços (incluindo a criação de sites do Microsoft IIS). Não altere suas configurações de serviço.

O Serviço de Telemetria Citrix está 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 por sua organização e estão completamente sob o controle do usuário, ou dispositivos de usuário que são gerenciados e administrados por 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 os 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 combata 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 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 a 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.

> **Observação:**
>
> Isso é típico de outros produtos de software; o uso de uma versão anterior do Active Directory impõe apenas 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 e XenDesktop 7.6 Feature Pack 2, a configuração de política **Permitir transferência de arquivo entre desktop e cliente** está habilitada no Site, mas não pode ser desabilitada por um Delivery Controller executando XenApp e 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 ao PC

O Acesso Remoto ao PC implementa os seguintes recursos de segurança:

- O uso de cartão inteligente é suportado.
- Quando uma sessão remota se conecta, o monitor do PC do escritório aparece em branco.
- O Acesso Remoto ao PC redireciona todas as entradas de teclado e mouse para a sessão remota, exceto CTRL+ALT+DEL e cartões inteligentes e dispositivos biométricos habilitados para USB.
- O SmoothRoaming é suportado apenas para um único usuário.
- Quando um usuário tem uma sessão remota conectada a um PC de escritório, apenas esse usuário pode retomar o acesso local ao PC do escritório. Para retomar o acesso local, o usuário pressiona Ctrl-Alt-Del no PC local e, em seguida, faz login com as mesmas credenciais usadas pela sessão remota. O usuário também pode retomar o acesso local inserindo um cartão inteligente ou utilizando biometria, se o seu sistema tiver a integração apropriada de Provedor de Credenciais de terceiros. Este comportamento padrão pode ser substituído ativando a Troca Rápida de Usuário (Fast User Switching) por meio de Objetos de Política de Grupo (GPOs) ou editando o registro.

Observação:

A Citrix recomenda que você não atribua privilégios de administrador de VDA a usuários de sessão gerais.

Atribuições automáticas

Por padrão, o Acesso Remoto ao PC suporta a atribuição automática de vários usuários a um VDA. No XenDesktop 5.6 Feature Pack 1, os administradores podiam substituir esse comportamento usando o script PowerShell RemotePCAccess.ps1. Esta versão usa uma entrada de registro para permitir ou proibir 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 exige 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 somente quando você tiver comunicações seguras entre seus Delivery Controllers e o 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.

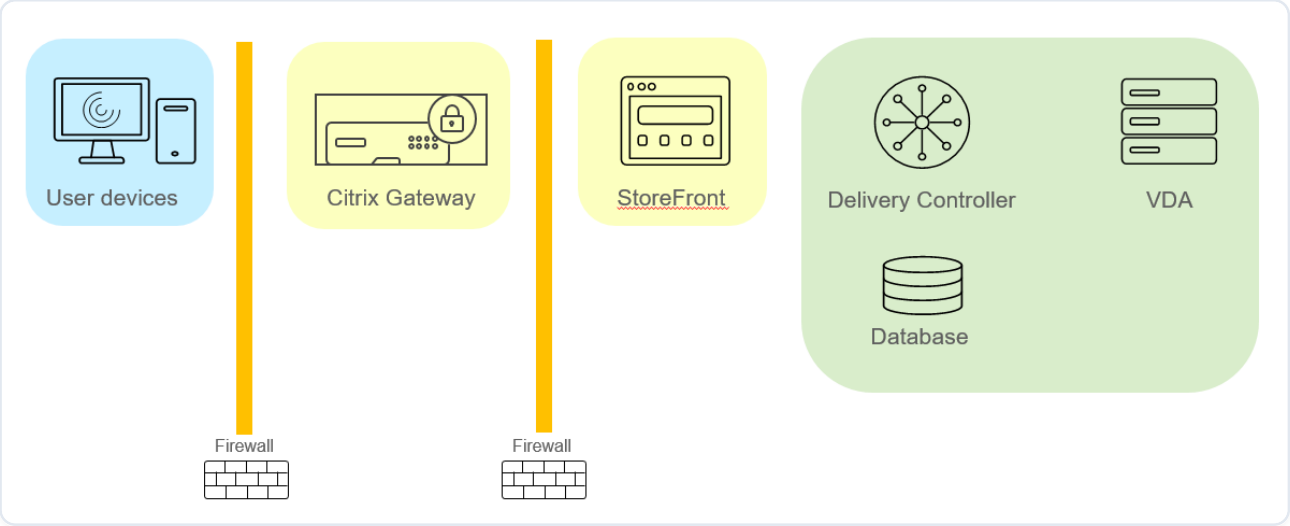
- Para verificar o valor atual da configuração de confiança XML, execute `Get-BrokerSite` e inspecione o valor de `TrustRequestsSentToTheXMLServicePort`.
- Para habilitar a confiança XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`.
- Para desabilitar a confiança XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`.

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 etapas de configuração detalhadas sobre como integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway, consulte a documentação do StoreFront.

O diagrama a seguir ilustra um exemplo de uma implantação simplificada da Citrix que inclui o Citrix Gateway. O Citrix Gateway se comunica com o StoreFront para proteger aplicativos e dados entregues pelo Citrix Virtual Apps and Desktops. Os dispositivos do usuário executam o aplicativo Citrix Workspace™ para criar uma conexão segura e acessar seus aplicativos, desktops e arquivos.



Os usuários fazem logon e autenticar usando o Citrix Gateway. O Citrix Gateway é implantado e protegido na DMZ. A autenticação de dois fatores é configurada. Com base nas credenciais do usuário, os usuários recebem os recursos e aplicativos relevantes. Aplicativos e dados estão em servidores apropriados (não mostrados no diagrama). Servidores separados são usados para aplicativos e dados sensíveis à segurança.

Administração delegada

O modelo de administração delegada oferece a flexibilidade para corresponder à forma como sua organização deseja delegar atividades de administração, usando controle baseado em função e objeto. A administração delegada acomoda implantações de todos os tamanhos e permite configurar mais granularidade de permissões à medida que sua implantação cresce em complexidade. A administração delegada usa três conceitos: administradores, funções e escopos.

- **Administradores:** Um administrador representa uma pessoa 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 internas ou personalizadas.

As funções integradas são:

FUNÇÃO	PERMISSÕES
Administrador Completo	Pode executar todas as tarefas e operações. Um Administrador Completo é sempre combinado com o escopo Todos.
Administrador Somente Leitura	Pode ver todos os objetos em escopos especificados, além de informações globais, mas não pode alterar nada. Por exemplo, um Administrador Somente Leitura com Escopo=Londres pode ver todos os objetos globais (como Registro de Configuração) e quaisquer objetos com escopo de Londres (por exemplo, Grupos de Entrega de Londres). No entanto, esse administrador não pode ver objetos no escopo de Nova York (assumindo que os escopos de Londres e Nova York não se sobreponham).
Administrador de Help Desk	Pode visualizar Grupos de Entrega e gerenciar as sessões e máquinas associadas a esses grupos. Pode ver o Catálogo de Máquinas e as informações do host para os Grupos de Entrega que estão sendo monitorados. Também pode 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. Essa função pode gerenciar imagens base e instalar software, mas não pode atribuir aplicativos ou desktops a usuários.

FUNÇÃO	PERMISSÕES
Administrador de Grupo de Entrega	Pode entregar aplicativos, desktops e máquinas; também pode gerenciar as sessões associadas. Também pode gerenciar configurações de aplicativos e desktops, como políticas e configurações de gerenciamento de energia.
Administrador de Host	Pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, aplicativos ou desktops a usuários.

Em certas edições do produto, você pode criar funções personalizadas para atender aos requisitos de sua organização e delegar permissões com mais detalhes. Você pode usar funções personalizadas para alocar permissões na granularidade de uma ação ou tarefa em um console.

- **Escopos:** Um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma relevante para sua organização (por exemplo, o conjunto de Grupos de Entrega 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 interno: 'Todos', que contém todos os objetos. A função de Administrador Completo é sempre emparelhada com o escopo Todos.

Exemplo

A Empresa XYZ decidiu gerenciar aplicativos e desktops com base em seu departamento (Contabilidade, Vendas e Armazém) e seu sistema operacional de desktop (Windows 7 ou Windows 8). O administrador criou cinco escopos e, em seguida, rotulou cada Grupo de Entrega com dois escopos: um para o departamento onde são usados e outro para o sistema operacional que utilizam.

Os seguintes administradores foram criados:

ADMINISTRADOR	FUNÇÕES	ESCOPOS
domain/fred	Administrador Completo	Todos (a função de Administrador Completo sempre tem o escopo Todos)

ADMINISTRADOR	FUNÇÕES	ESCOPOS
domain/rob	Administrador Somente Leitura	Todos
domain/heidi	Administrador Somente Leitura, Administrador de Suporte Técnico	Todas as Vendas
domain/warehouseadmin	Administrador de Help Desk	Armazém
domain/peter	Administrador de Grupo de Entrega, Administrador de Catálogo de Máquinas	Win7

- Fred é um Administrador Completo e pode visualizar, editar e excluir todos os objetos no sistema.
- Rob pode visualizar todos os objetos no site, mas não pode editá-los ou excluí-los.
- Heidi pode visualizar todos os objetos e pode realizar tarefas de help desk 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 help desk 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 pode entregar aplicativos, desktops e máquinas do Windows 7, independentemente do escopo do departamento em que estejam. A administradora considerou tornar Peter um Administrador Completo para o escopo Win7. No entanto, ela decidiu contra isso, porque um Administrador Completo também tem direitos totais sobre todos os objetos que não estão no escopo, como 'Site' e 'Administrador'.

Como usar a administração delegada

Geralmente, o número de administradores e a granularidade de suas permissões dependem do tamanho e da complexidade da implantação.

- Em implantações pequenas ou de prova de conceito, um ou poucos administradores fazem tudo. Não há delegação. Neste caso, crie cada administrador com a função interna de Administrador Completo, 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 Help Desk. 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 internas e os escopos apropriados.
- Implantações ainda maiores podem exigir mais (ou mais específicos) escopos, 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 interna 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

Ao criar um site como administrador local, sua conta de usuário se torna automaticamente um Administrador Completo com permissões totais sobre todos os objetos. Após a criação de um site, 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 funções de administração até mais tarde. Para administradores habilitados existentes, você pode querer desabilitar vários deles enquanto reorganiza seus objetos/escopos e, em seguida, reabilitá-los quando estiver pronto para entrar em operação com a configuração atualizada. Você não pode desabilitar um Administrador Completo se isso resultar na ausência de um Administrador Completo habilitado. A caixa de seleção habilitar/desabilitar está disponível ao criar, copiar ou editar um administrador.

Ao excluir um par função/escopo ao copiar, editar ou excluir um administrador, ele exclui apenas o relacionamento entre a função e o escopo para esse administrador. Ele não exclui a função nem o escopo. Também não afeta nenhum outro administrador que esteja configurado com esse par função/escopo.

Para gerenciar administradores, clique em **Configuração > Administradores** no painel de navegação do Studio e, em seguida, clique na guia **Administradores** no painel superior central.

- **Criar um administrador:** Clique em **Criar novo Administrador** no painel Ações. Digite ou navegue até o nome da conta de usuário, selecione ou crie um escopo e selecione uma função. O novo administrador é habilitado por padrão; você pode alterar isso.
- **Copiar um administrador:** Selecione o administrador no painel central e, em seguida, clique em **Copiar Administrador** no painel Ações. Digite ou navegue até 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 no painel central e, em seguida, clique em **Editar Administrador** no painel Ações. Você pode editar ou excluir qualquer um dos pares função/escopo e adicionar novos.
- **Excluir um administrador:** Selecione o administrador no painel central e, em seguida, clique em **Excluir Administrador** no painel 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 de função e escopo associados ao administrador contêm funções ou escopos inutilizáveis. A seguinte mensagem de aviso aparece se um par de função e escopo associado contiver funções ou escopos inutilizáveis:

- Função ou escopo associado não utilizável
    - Remova o par de função e escopo do administrador.

> **Importante:**
>
> Uma mensagem de aviso aparece apenas quando um par de função e escopo associado contém funções ou escopos inutilizáveis, ou ambos.
>
> Para remover o par de função e escopo do administrador, conclua uma das seguintes etapas:

- Exclua o par função e escopo.

    a. No painel **Ações**, clique em **Editar Administrador**.

b. Na janela **Editar Administrador**, selecione o par de função e escopo e clique em **Excluir**.

c. Clique em **OK** para sair.

- Exclua o administrador.

a. No painel **Ações**, clique em **Excluir Administrador**.

b. Na janela **Studio**, 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 no painel Ações.

> Para gerenciar funções, clique em **Configuração > Administradores** no painel de navegação do Studio e, em seguida, clique na guia **Funções** no painel superior central.

- **Exibir detalhes da função:** Selecione a função no painel central. A parte inferior do painel central lista os tipos de objeto e as permissões associadas à função. Clique na guia Administradores no painel inferior para exibir uma lista de administradores que atualmente têm essa função.
- **Criar uma função personalizada:** Clique em **Criar nova função** no painel Ações. Insira um nome e uma descrição. Selecione os tipos de objeto e as permissões.

- **Copiar uma função:** Selecione a função no painel central e clique em **Copiar função** no painel Ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
- **Editar uma função personalizada:** Selecione a função no painel central e clique em **Editar função** no painel Ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
- **Excluir uma função personalizada:** Selecione a função no painel do meio e clique em **Excluir Função** no painel 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 Delivery Groups associados.

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 podem conter até 256 caracteres Unicode.

Ao copiar ou editar um escopo, lembre-se de que a remoção de objetos do escopo pode tornar esses objetos inacessíveis ao administrador. Se o escopo editado for emparelhado com uma ou mais funções, certifique-se de que as atualizações do escopo não tornem nenhum par de função/escopo inutilizável.

Para gerenciar escopos, clique em **Configuração > Administradores** no painel de navegação do Studio e, em seguida, clique na guia **Escopos** no painel superior do meio.

- **Criar um escopo:** Clique em **Criar novo Escopo** no painel Ações. Insira um nome e uma descrição. Para incluir todos os objetos de um tipo específico (por exemplo, Delivery Groups), selecione o tipo de objeto. Para incluir objetos específicos, expanda o tipo e selecione objetos individuais (por exemplo, Delivery Groups usados pela equipe de Vendas).
- **Copiar um escopo:** Selecione o escopo no painel do meio e clique em **Copiar Escopo** no painel Ações. Insira um nome e uma descrição. Altere os tipos de objeto e os objetos, conforme necessário.
- **Editar um escopo:** Selecione o escopo no painel do meio e clique em **Editar Escopo** no painel Ações. Altere o nome, a descrição, os tipos de objeto e os objetos, conforme necessário.
- **Excluir um escopo:** Selecione o escopo no painel do meio e clique em **Excluir Escopo** no painel 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 de função/escopo associados a um administrador, além das permissões individuais para cada tipo de objeto (por exemplo, Delivery Groups e Catálogos de Máquinas). Você gera este relatório a partir do Studio.

  Para criar este relatório, clique em **Configuração > Administradores** no painel de navegação do Studio. Selecione um administrador no painel central e, em seguida, clique em **Criar Relatório** no painel 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
```

Em um prompt de comando do Windows, o comando de exemplo anterior é:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

Gerenciar chaves de segurança

Nota:

- Você deve usar este recurso em combinação com o StoreFront™ 1912 LTSR CU2 ou posterior.
- O recurso Secure XML é compatível apenas com Citrix ADC e Citrix Gateway versão 12.1 e posterior.

Este recurso permite que apenas máquinas StoreFront e Citrix Gateway aprovadas se comuniquem com os Citrix Delivery Controllers. Depois de habilitar este recurso, todas as solicitações que não contiverem a chave serão bloqueadas. Use este recurso para adicionar uma camada extra de segurança para proteger contra ataques originados da rede interna.

Um fluxo de trabalho geral para usar este recurso é o seguinte:

1. Habilite o Studio para mostrar as configurações do recurso.
2. Configure as definições para o seu site.
3. Configure as definições no StoreFront.
4. Configure as configurações no Citrix ADC.

Habilitar o Studio para mostrar as configurações do recurso

Por padrão, as configurações das chaves de segurança estão ocultas no Studio. Para habilitar o Studio a exibi-las, use o PowerShell SDK da seguinte forma:

1. Execute o PowerShell SDK do Citrix Virtual Apps and Desktops™.
2. Em uma janela de comando, execute os seguintes comandos:
   - `Add-PSSnapIn Citrix*`. Este comando adiciona os snap-ins do Citrix.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

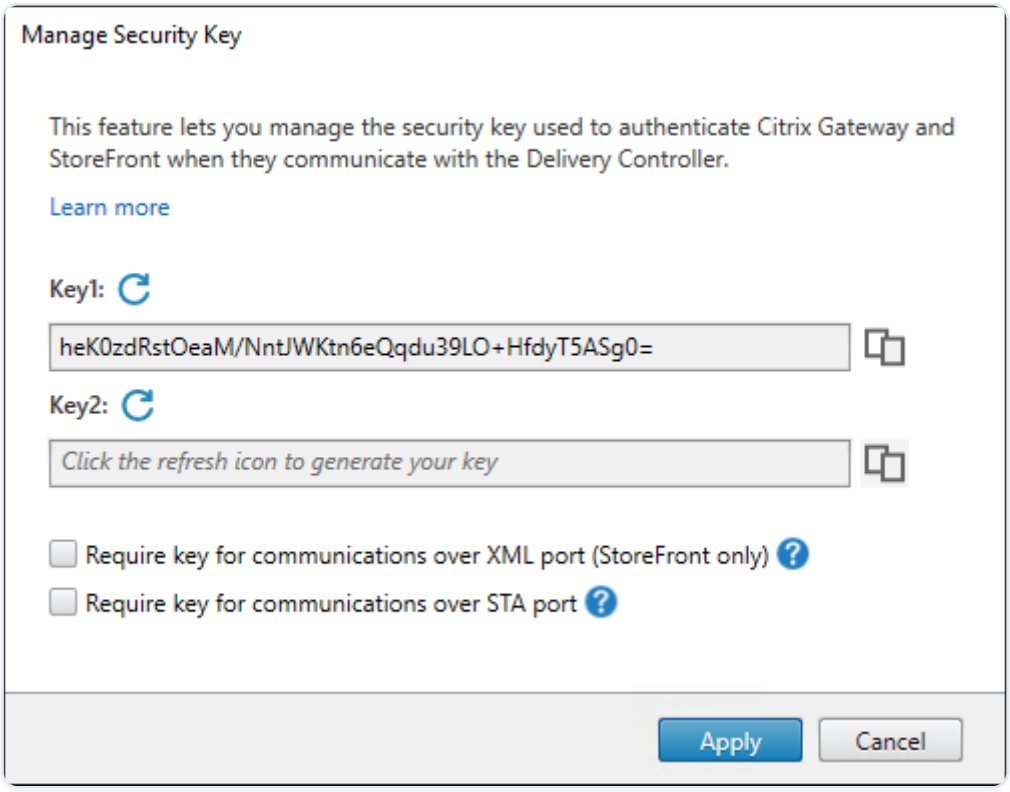
Para obter mais informações sobre o PowerShell SDK, consulte SDKs e APIs.

Configurar definições para o site

Você pode usar o Studio ou o PowerShell para configurar as definições da chave de segurança para o seu site.

Usar o console do Studio

1. navegar para **Studio > Settings > Manage security key** e clique em **Edit**. A janela **Manage Security Key** é exibida.



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.

2. Clique no ícone de atualização para gerar novas chaves.
3. Selecione onde uma chave é necessária:
   - **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.
4. Clique em **Save** para aplicar suas alterações e sair da janela.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações do 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 no StoreFront

Após concluir a configuração do seu site, você precisa configurar as definições relevantes no StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos PowerShell:

Para configurar a chave para comunicações pela porta XML, use o comando . Por exemplo:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Insira os valores apropriados para os seguintes parâmetros:

- `Path to store`
- `Resource feed name`
- `secret`

Para configurar a chave para comunicações sobre a porta STA, use os comandos `New-STFSecureTicketAuthority` e `Set-STFRoamingGateway`. Por exemplo:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]
```

```
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Insira os valores apropriados para os seguintes parâmetros:

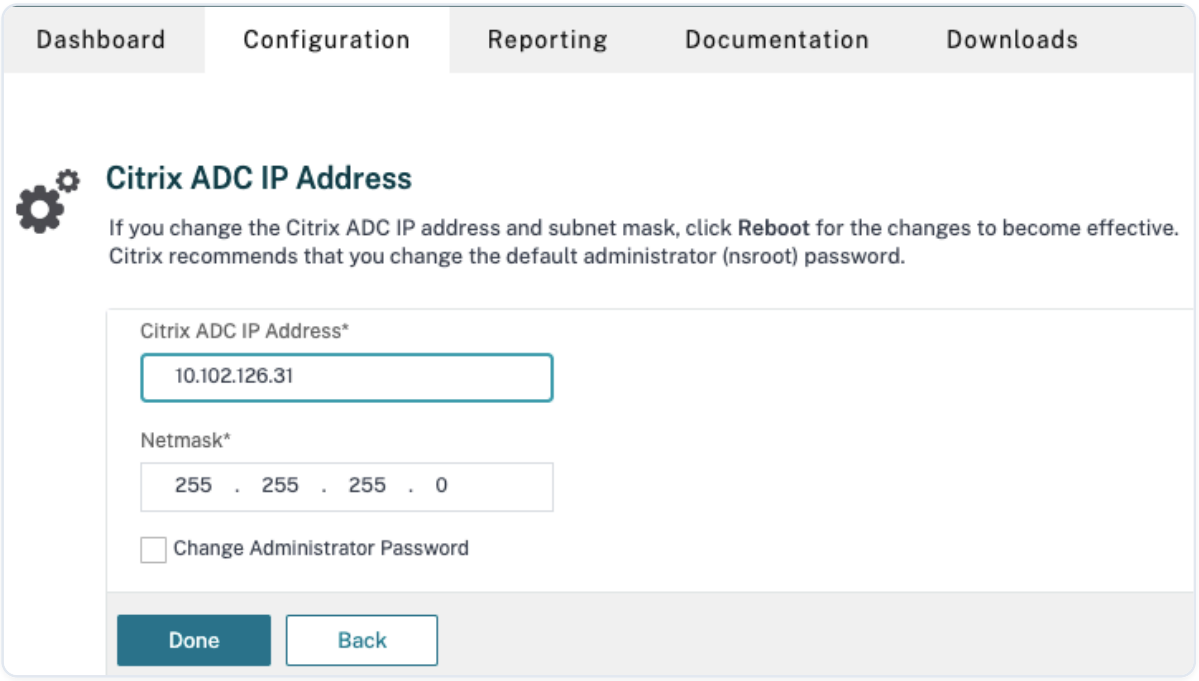
- `Gateway name`
- `STA URL`
- `Secret`

Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

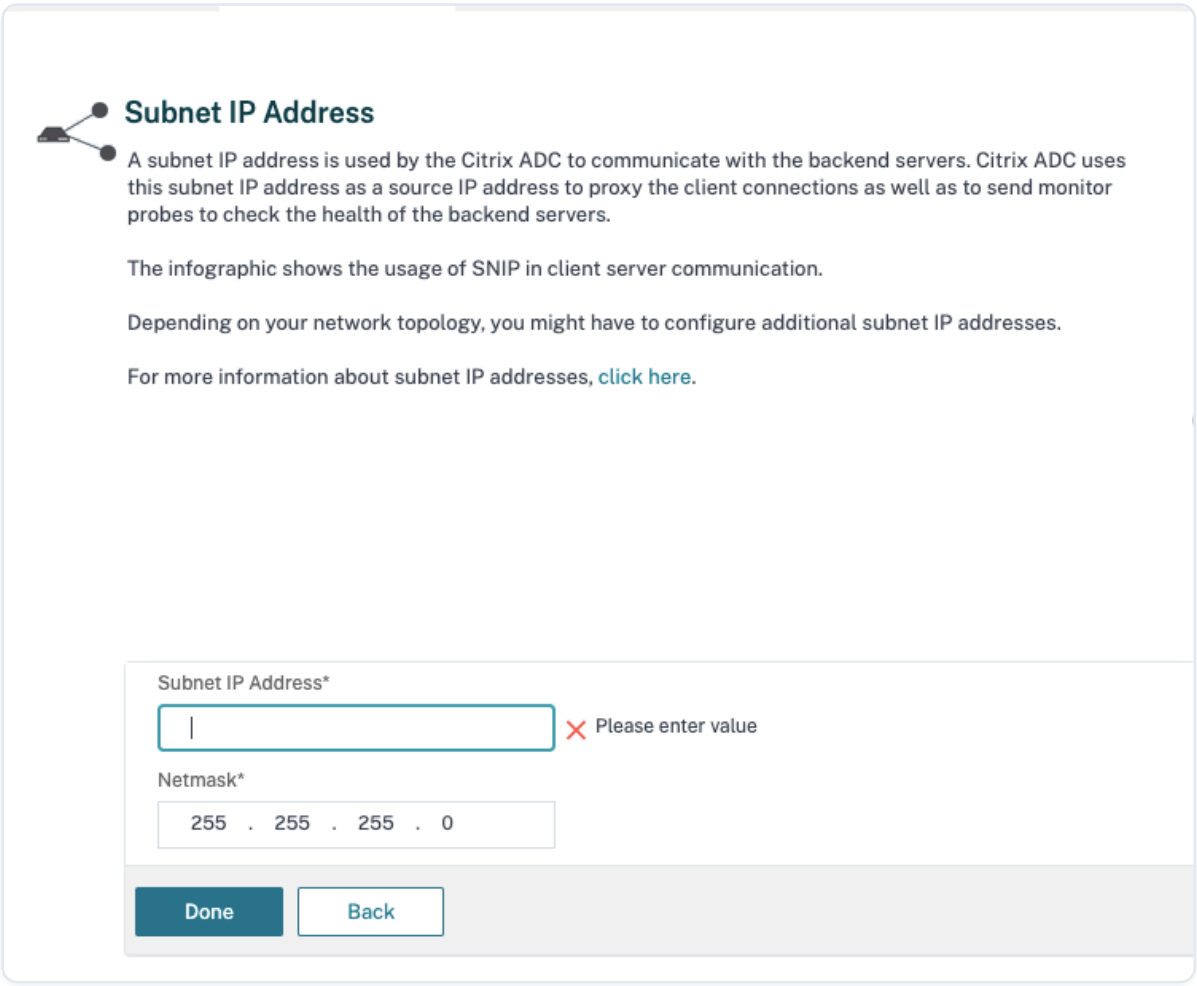
Configurar definições no Citrix ADC

> **Nota:**
>
> A configuração desse recurso no Citrix ADC não é necessária, a menos que você use o Citrix ADC como seu gateway. Se você usar o Citrix ADC, siga as etapas abaixo.

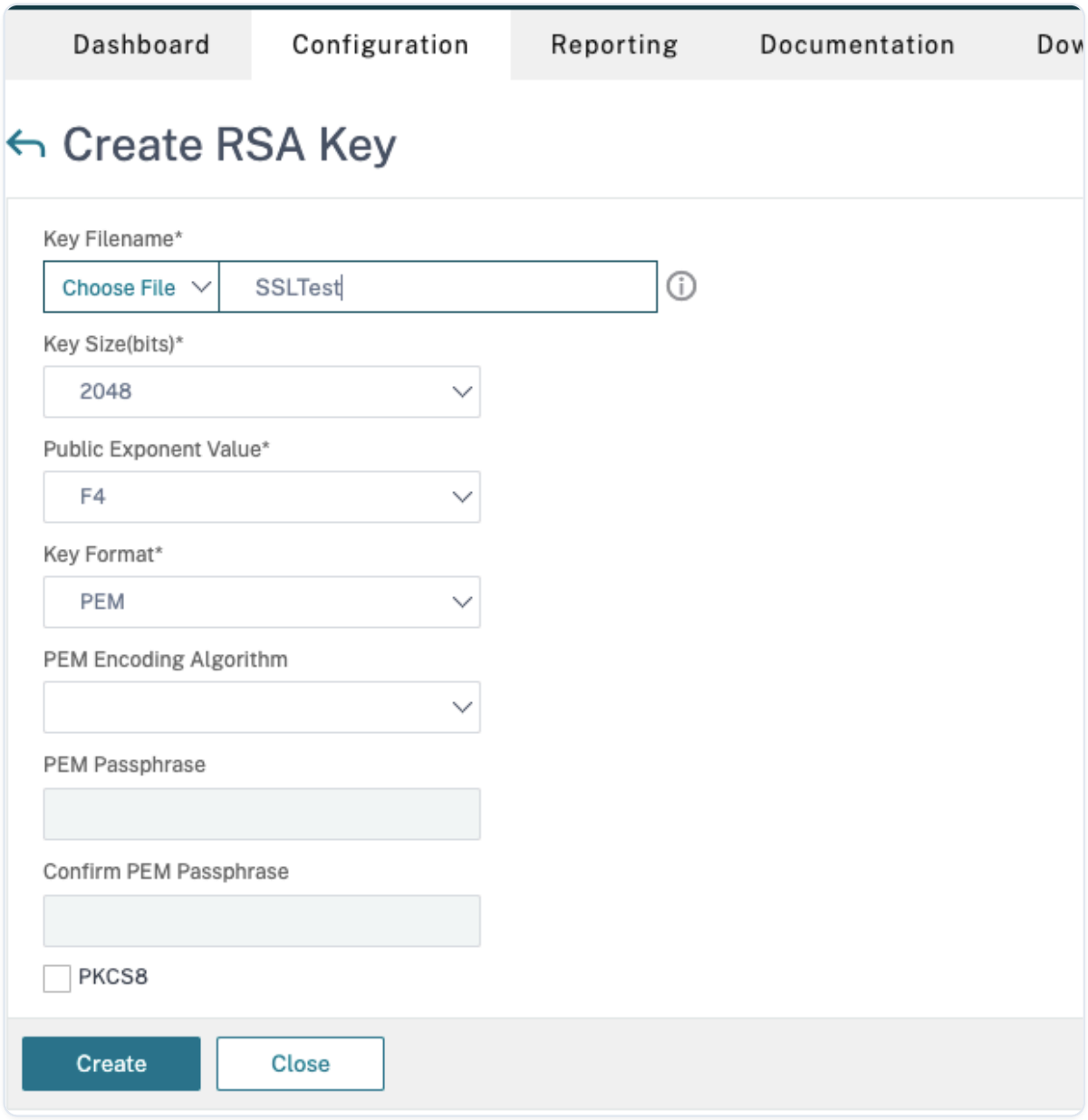
1. Certifique-se de que a seguinte configuração de pré-requisito já esteja em vigor:
    - Os seguintes endereços IP relacionados ao Citrix ADC estão configurados.
        - Endereço IP de Gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



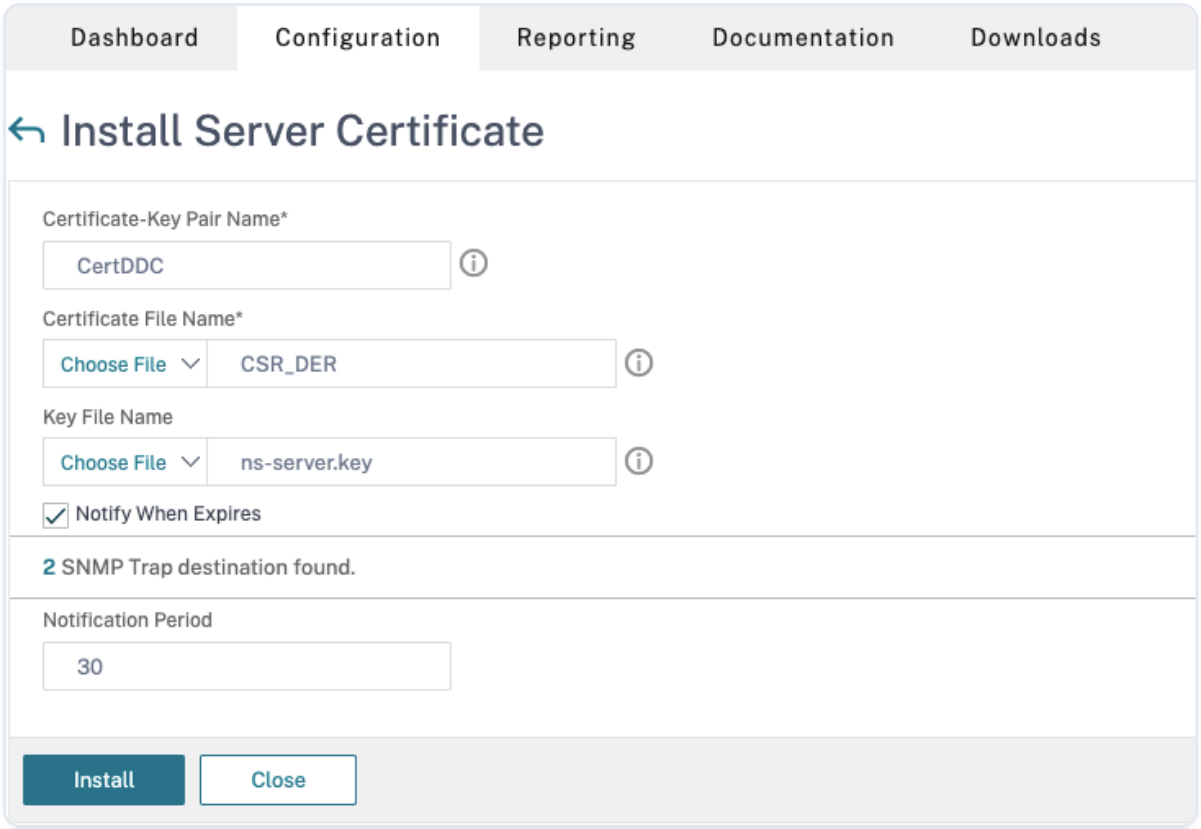
- Endereço IP de sub-rede (SNIP) para habilitar a comunicação entre o dispositivo Citrix ADC e os servidores de back-end. Para obter detalhes, consulte Configuring Subnet IP Addresses.
- Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no dispositivo ADC para o lançamento da sessão. Para obter detalhes, consulte Create a virtual server.

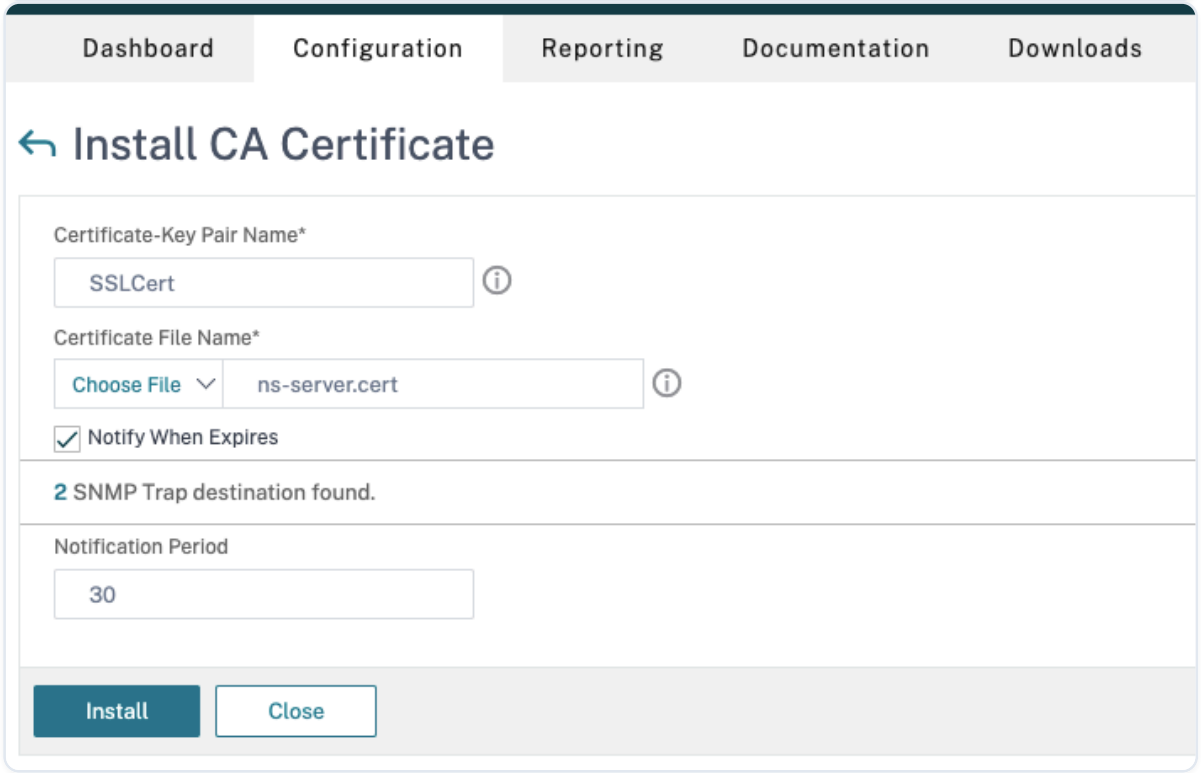


- Os modos e recursos necessários no dispositivo Citrix ADC estão habilitados.
  - Para habilitar os modos, na GUI do Citrix ADC, navegar até **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, navegar até **System > Settings > Configure Basic Features**.
- As configurações relacionadas a certificados estão concluídas.
  - A Solicitação de Assinatura de Certificado (CSR) é criada. Para obter detalhes, consulte Create a certificate.

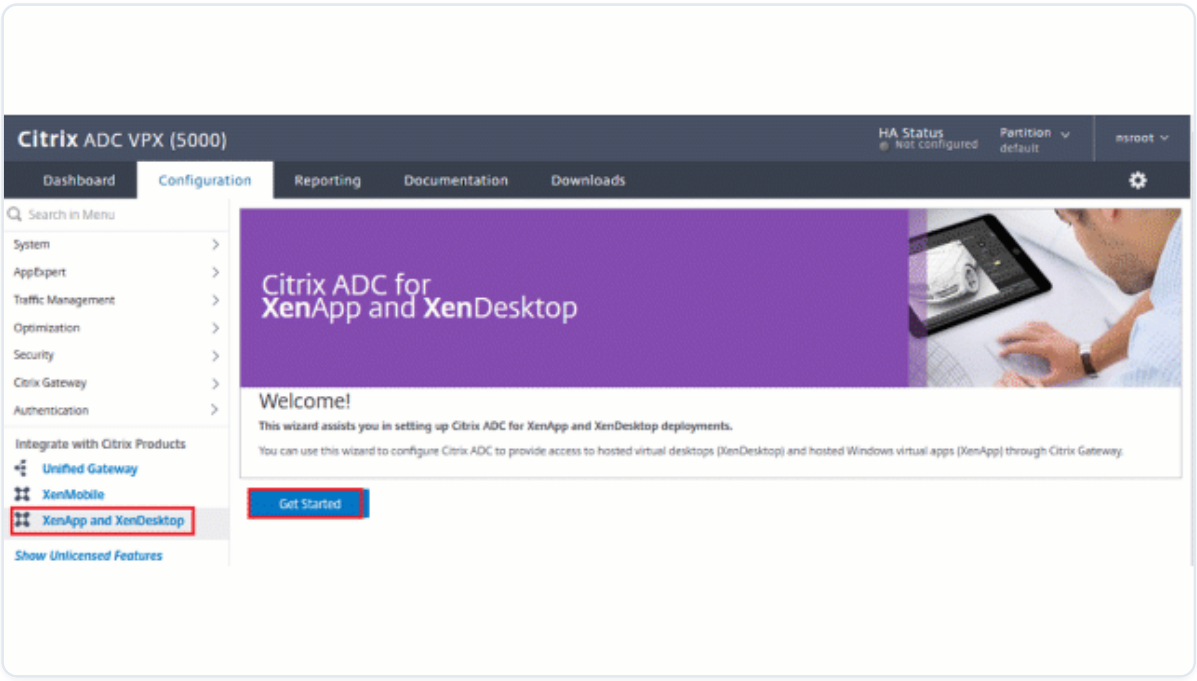


- Os certificados de servidor e CA e os certificados raiz são instalados. Para obter detalhes, consulte Install, link, and updates.





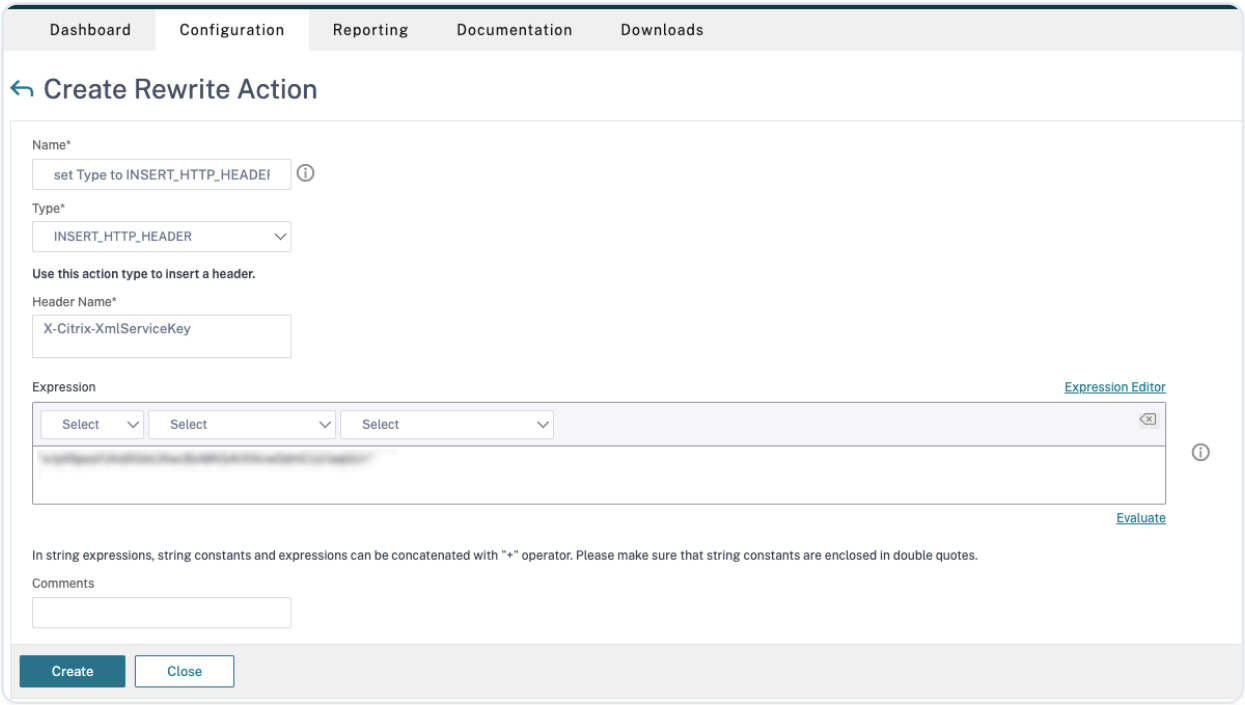
- Um Citrix Gateway foi criado para o Citrix Virtual Desktops. Teste a conectividade clicando no botão **Testar Conectividade STA** para confirmar que os servidores virtuais estão online. Para obter detalhes, consulte Configurando o Citrix ADC para Citrix Virtual Apps and Desktops.



2. Adicione uma ação de reescrita. Para obter detalhes, consulte Configuring a Rewrite Action.

   a. navegar até **AppExpert > Rewrite > Actions**.

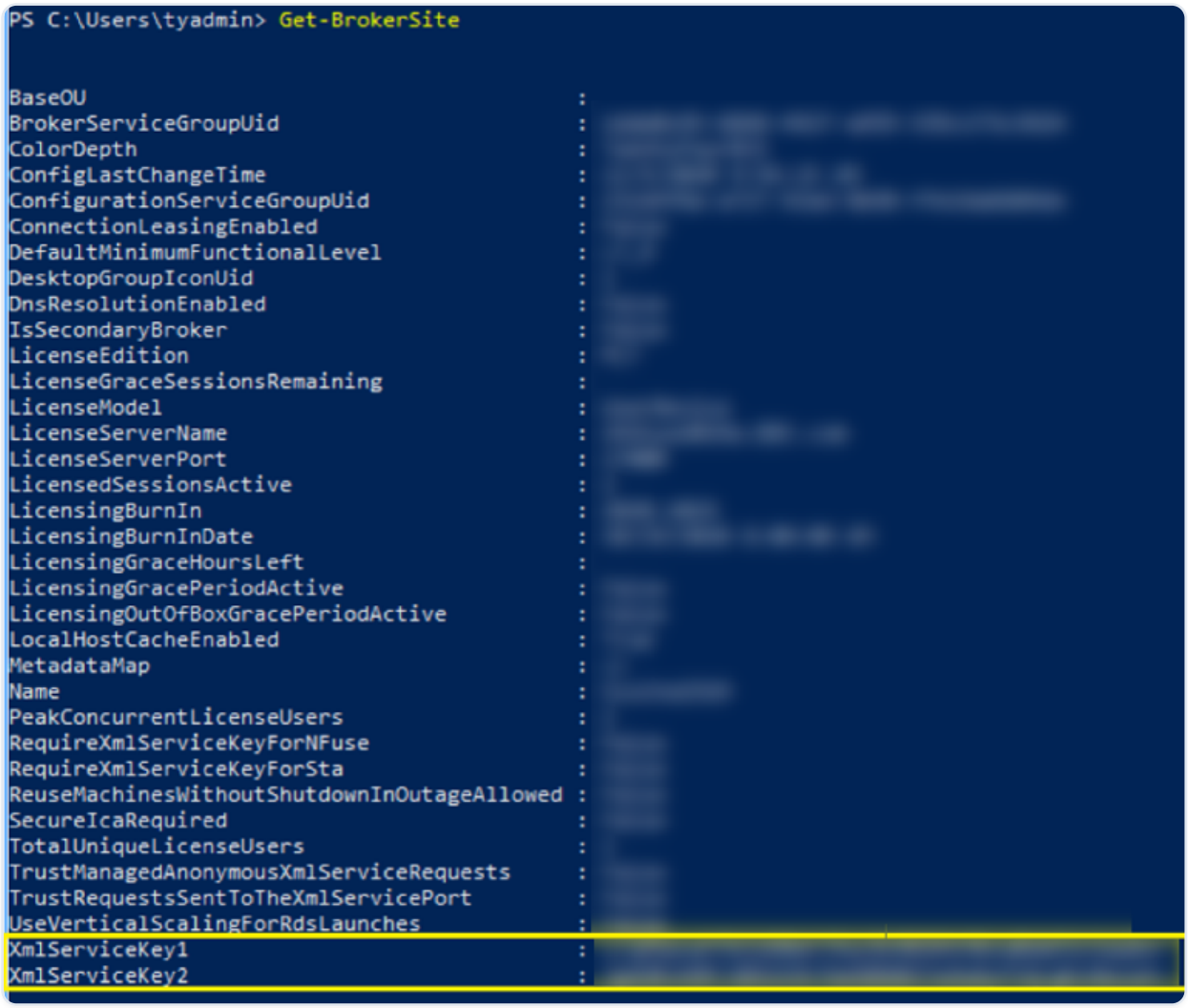
   b. Clique em **Adicionar** para adicionar uma nova ação de reescrita. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".



   a. Em **Tipo**, selecione **INSERT_HTTP_HEADER**.

   b. Em **Nome do Cabeçalho**, insira X-Citrix-XmlServiceKey.

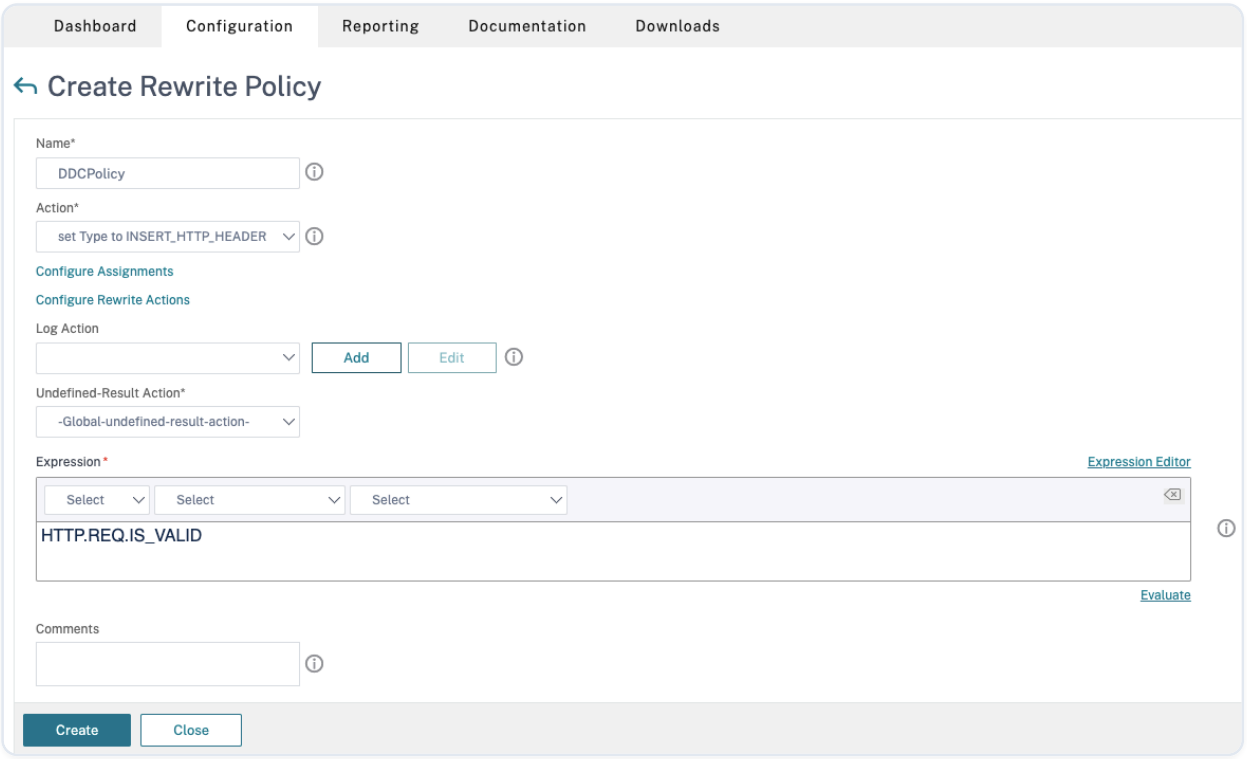
   c. Em **Expressão**, adicione `<XmlServiceKey1 value>` com as aspas. Você pode copiar o valor XmlServiceKey1 da sua configuração do Desktop Delivery Controller™.



3. Adicione uma política de reescrita. Para obter detalhes, consulte Configurando uma Política de Reescrita.

   a. navegar até **AppExpert > Rewrite > Policies**.

   b. Clique em **Add** para adicionar uma nova política.



a. Em **Action**, selecione a ação criada na etapa anterior.

b. Em **Expression**, adicione HTTP.REQ.IS_VALID.

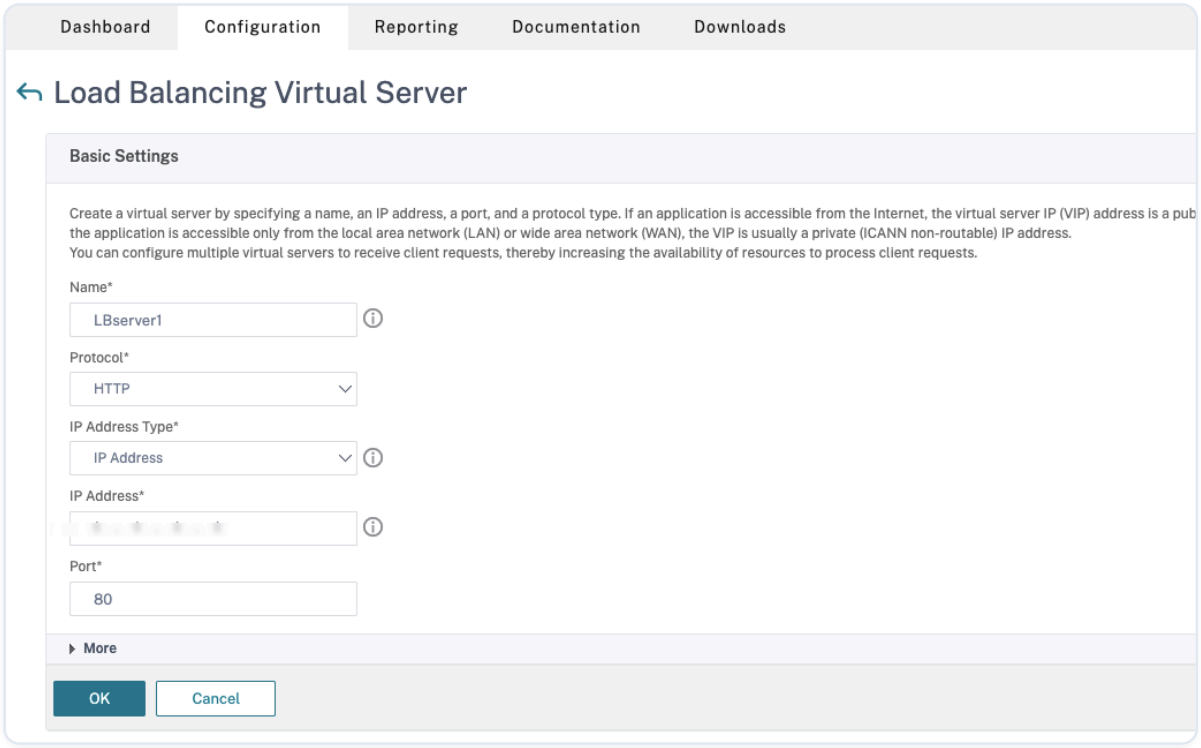
c. Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões não serão iniciadas.

   Para obter detalhes, consulte Configurar balanceamento de carga básico.

   a. Crie um servidor virtual de balanceamento de carga.

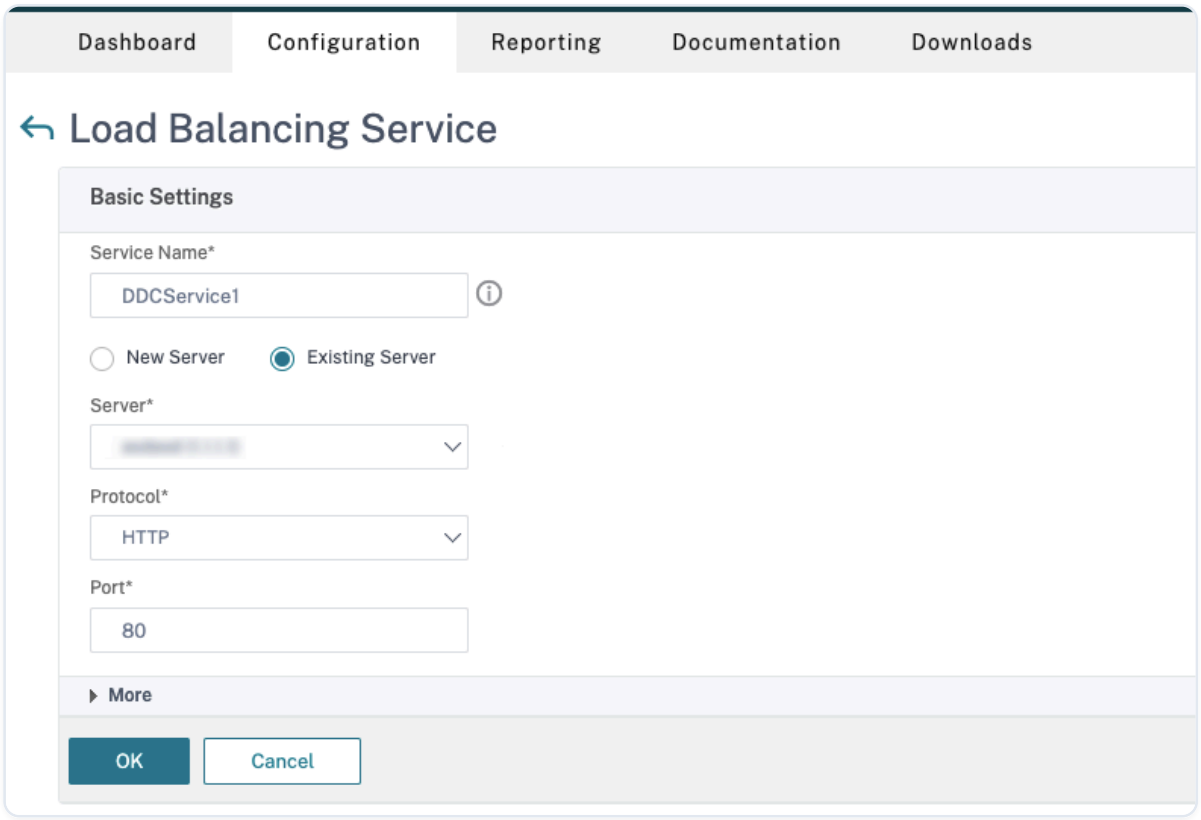
      - navegar até **Traffic Management > Load Balancing > Servers**.
      - Na página **Virtual Servers**, clique em **Adicionar**.



- 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.

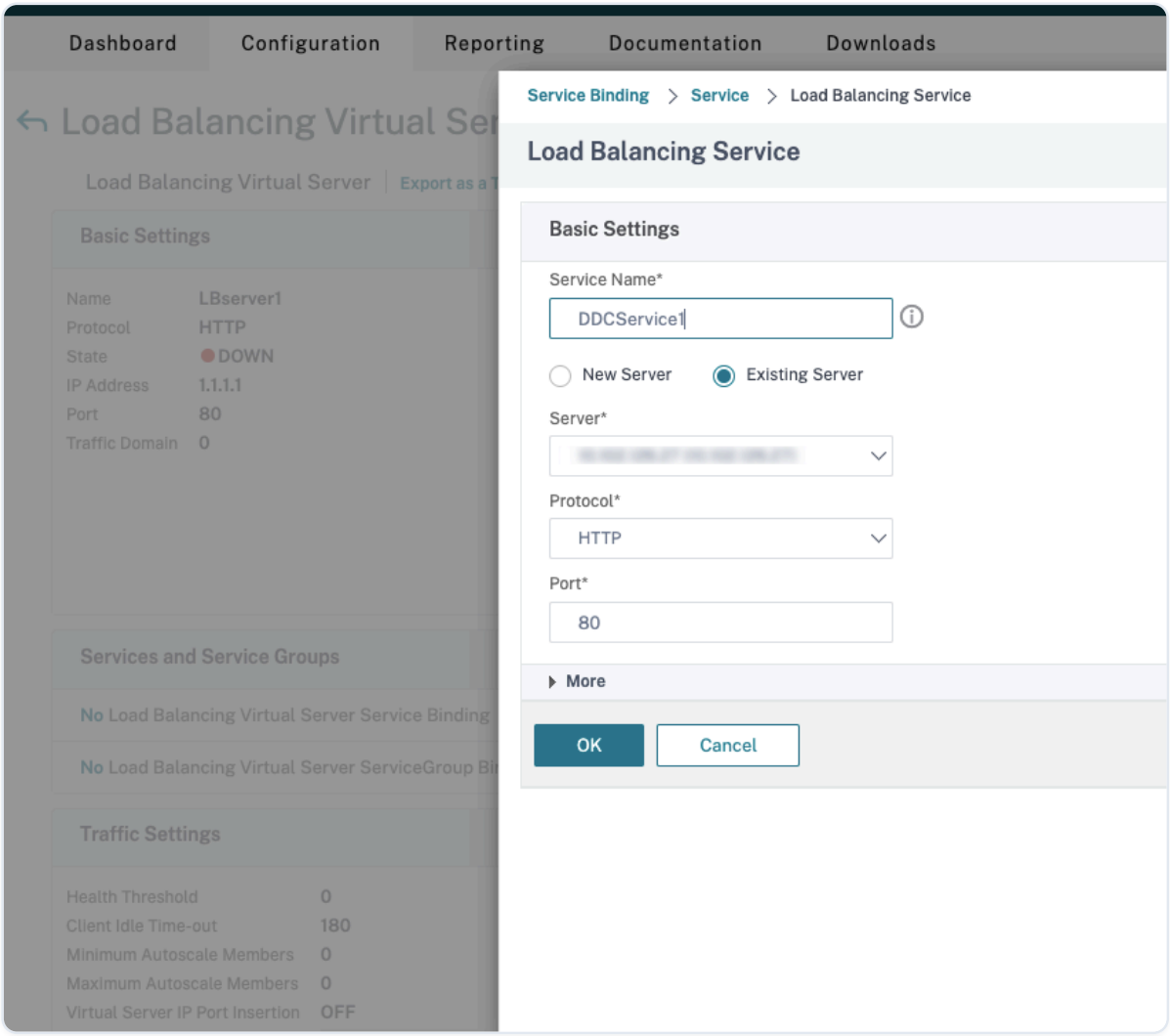
- navegar até **Traffic Management > Load Balancing > Services**.



- Em **Existing Server**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocol**, selecione **HTTP** e em **Port**, selecione **80**.
- Clique em **OK** e, em seguida, clique em **Done**.

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**.

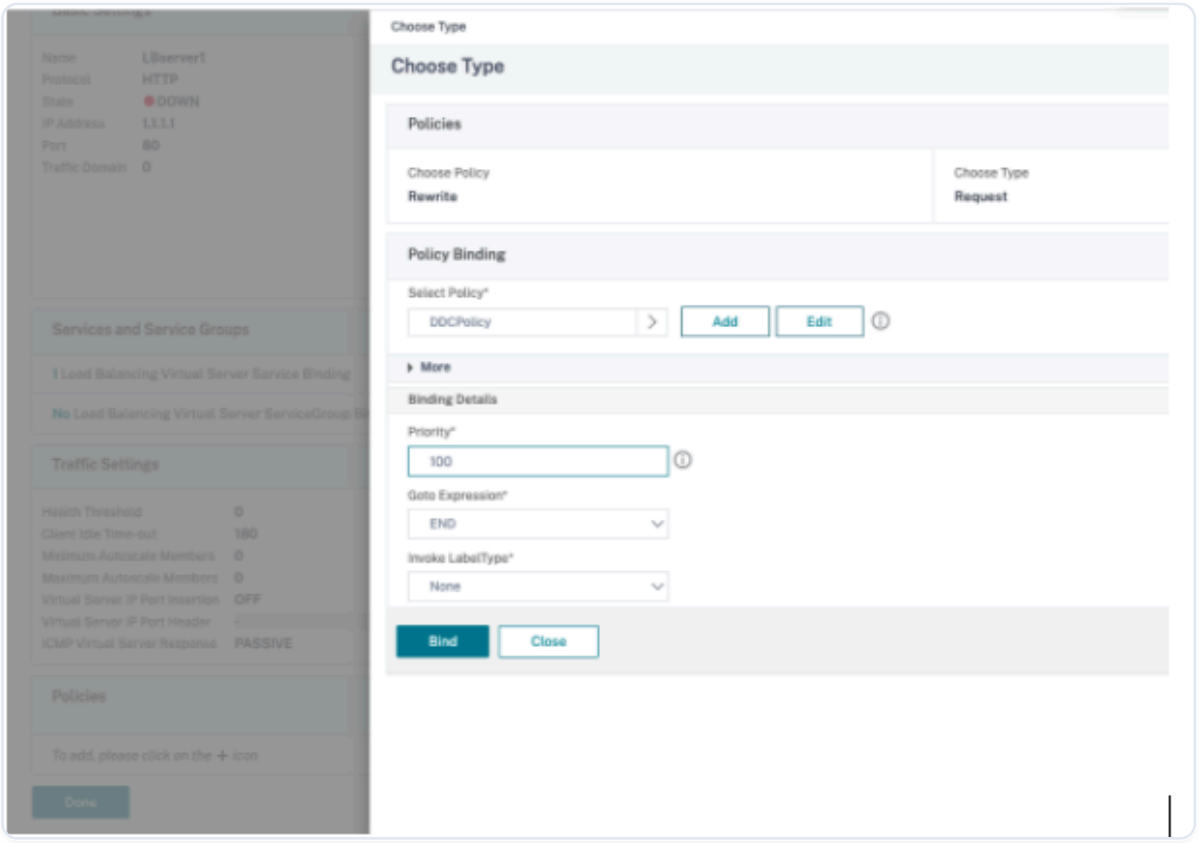


- Em **Service Binding**, selecione o serviço criado anteriormente.
- Clique em **Vincular**.

d. Vincule a política de reescrita criada anteriormente ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.

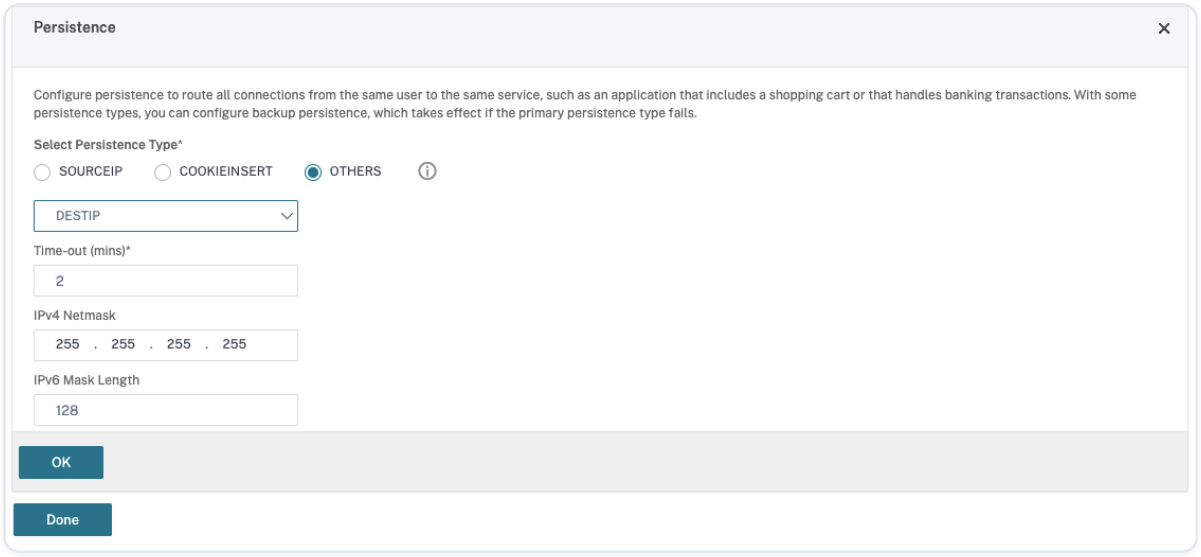
- Em **Configurações Avançadas**, clique em **Políticas,** e, em seguida, na seção **Políticas**, clique em **+**.



- 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 uma máscara de rede igual à do DDC.
- Clique em **OK**.

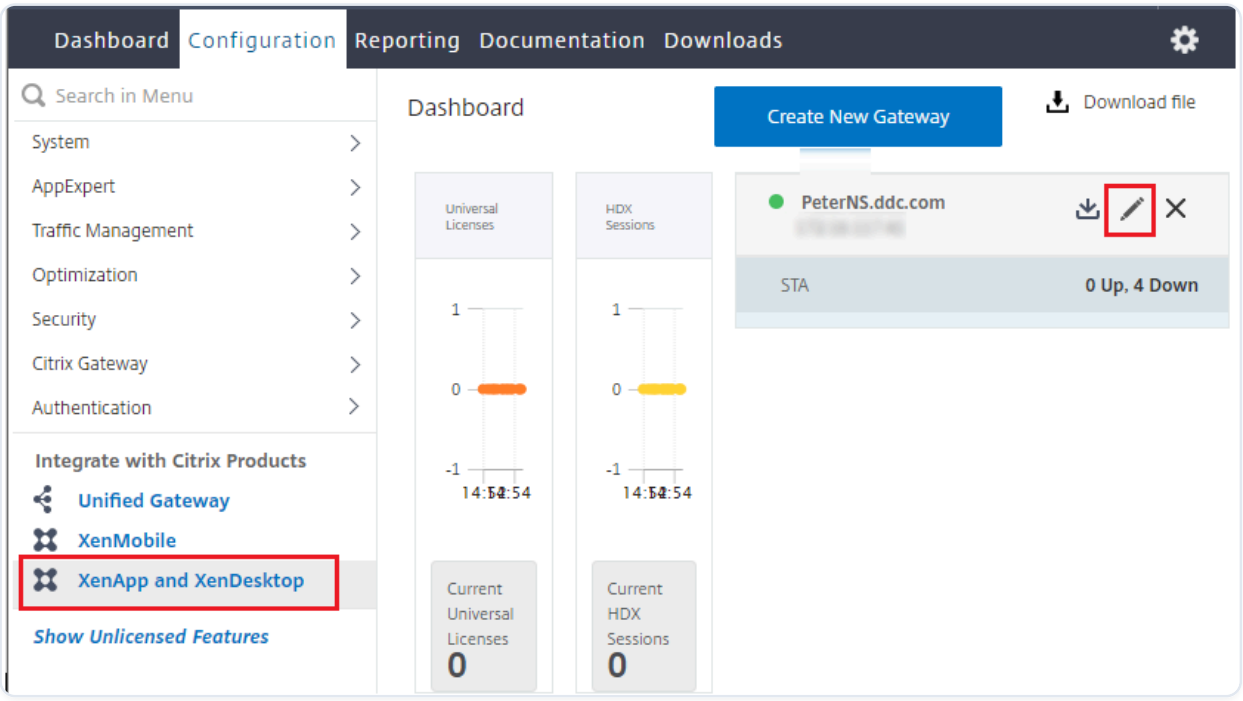
f. Repita estas etapas para o outro servidor virtual também.

Alterações de configuração se o dispositivo Citrix ADC já estiver configurado com Citrix Virtual Desktops™

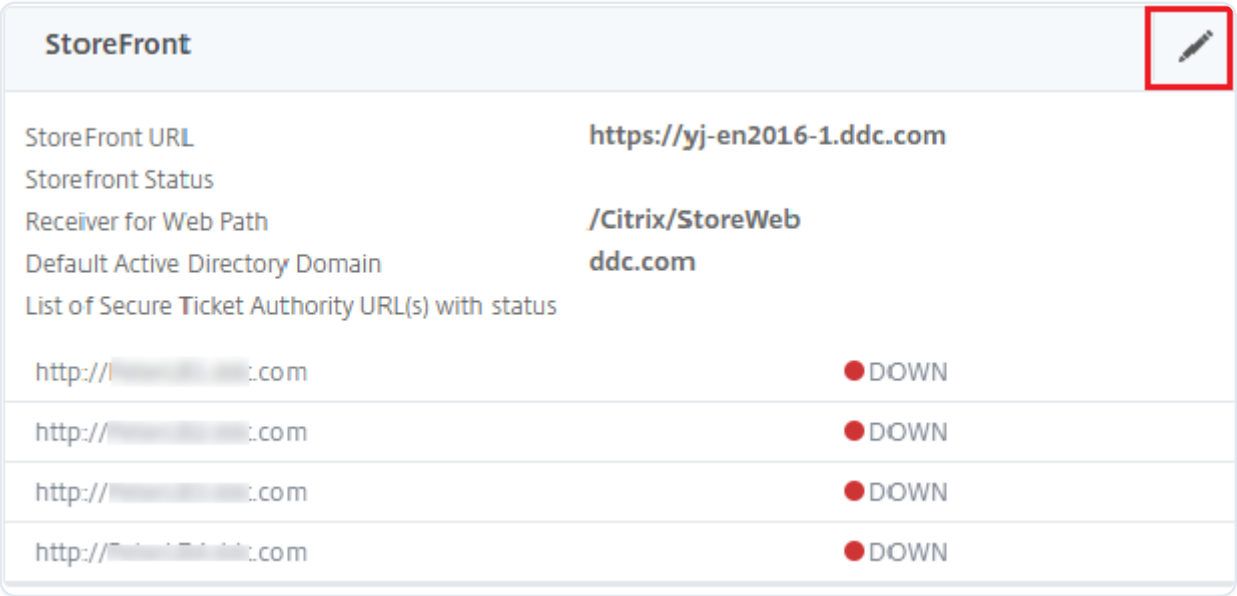
Se você já configurou o dispositivo Citrix ADC com Citrix Virtual Desktops, então, para usar o recurso Secure XML, você deve fazer as seguintes alterações de configuração.

- 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 Citrix Virtual Desktops, então o `TrustRequestsSentToTheXmlServicePort` é definido como True.

1. Na GUI do Citrix ADC, navegar para **Configuration > Integrate with Citrix Products** e clique em **XenApp and XenDesktop®**.
2. Selecione a instância do gateway e clique no ícone de edição.

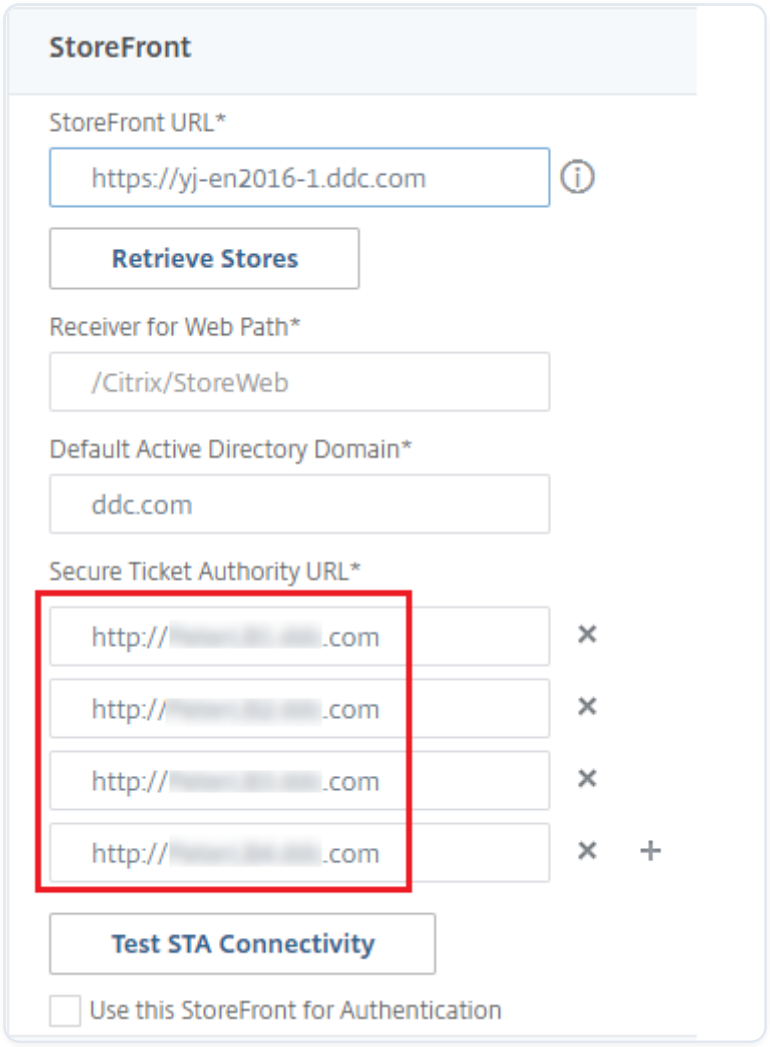


3. No painel StoreFront, clique no ícone de edição.



4. Adicione 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.



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™:

- Entenda 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 consumo 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 como suportar 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 pelo Microsoft Windows Hardware Quality Labs (WHQL) para serem usados em computadores que executam sistemas operacionais Windows qualificados. Consulte a documentação da Microsoft para obter informações adicionais sobre a conformidade de hardware PC/SC. Outros tipos de dispositivos de usuário podem estar em conformidade com o padrão PS/SC. Para obter mais informações, consulte o programa Citrix Ready.

Geralmente, é necessário um driver de dispositivo separado para o cartão inteligente de cada fornecedor ou equivalente. No entanto, se os cartões inteligentes estiverem em conformidade com um padrão como o NIST Personal Identity Verification (PIV), pode ser possível usar um único driver de dispositivo para uma variedade de cartões inteligentes. O driver do dispositivo deve ser instalado tanto no dispositivo do usuário quanto no Virtual Delivery Agent (VDA). O driver do 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 do dispositivo também pode ser descrito como um Cryptographic Service Provider (CSP), Key Storage Provider (KSP) ou minidriver.

As seguintes combinações de cartão inteligente e middleware para sistemas Windows foram testadas pela Citrix como exemplos representativos de seu tipo. No entanto, outros cartões inteligentes e middleware também podem ser usados. Para obter mais informações sobre cartões inteligentes e middleware compatíveis com Citrix, consulte `<http://www.citrix.com/ready>`.

MIDDLEWARE	CARTÕES CORRESPONDENTES
Mini Driver Gemalto para cartão .NET	Gemalto .NET v2+

Para obter informações sobre o uso de cartões inteligentes com outros tipos de dispositivos, consulte a documentação do aplicativo Citrix Workspace™ para esse dispositivo.

Acesso Remoto ao PC

Os cartões inteligentes são suportados apenas para acesso remoto a PCs físicos de escritório que executam Windows 10, Windows 8 ou Windows 7.

Os seguintes cartões inteligentes foram testados com o Acesso Remoto ao 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 com alta latência. Quando a latência é alta, a melhoria de desempenho pode ser significativa (por exemplo, 15 segundos para um logon de cartão inteligente rápido do Windows em comparação com mais de 1 minuto com o redirecionamento de cartão inteligente baseado em PC/SC).

O cartão inteligente rápido é habilitado por padrão em máquinas host com VDAs do 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 habilitar ou forçado a desabilitar (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:

- Somente 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 da versão 2203 do VDA e da versão 2202 do aplicativo Citrix Workspace para Windows (ou posterior), o cartão inteligente rápido é compatível com 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 seu 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 seu 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** está desativado por padrão. Ele pode ser ativado e controlado com as seguintes configurações de registro no VDA:

Em HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` como um DWORD (não-zero para ativar)
- `EnableLogonPinSessionCache` como um DWORD (não-zero para ativar)
- `PinSessionCacheEntryStaleTimeout` como um DWORD (número de segundos antes que uma entrada se torne obsoleta, o padrão é 1 hora)

Tipos de leitores de cartão inteligente

Um leitor de cartão inteligente pode ser integrado ao dispositivo do usuário ou ser conectado 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 leitor onde o usuário insere o cartão inteligente. O padrão Deutsche Kreditwirtschaft (DK) define quatro classes de leitores de cartão de contato.

- Os leitores de cartão inteligente Classe 1 são os mais comuns e geralmente contêm um slot. Os leitores de cartão inteligente Classe 1 são suportados, geralmente com um driver de dispositivo CCID padrão fornecido com o sistema operacional.
- Os leitores de cartão inteligente Classe 2 também contêm um teclado seguro que não pode ser acessado pelo dispositivo do usuário. Os leitores de cartão inteligente Classe 2 podem ser integrados a um teclado com um teclado seguro integrado. Para leitores de cartão inteligente Classe 2, entre em contato com seu representante Citrix; um driver de dispositivo específico do leitor pode ser necessário para habilitar a capacidade de teclado seguro.
- Os leitores de cartão inteligente Classe 3 também contêm um display seguro. Os leitores de cartão inteligente Classe 3 não são suportados.
- Os leitores de cartão inteligente Classe 4 também contêm um módulo de transação seguro. Os leitores de cartão inteligente Classe 4 não são suportados.

> **Observação:**
>
> A classe do leitor de cartão inteligente não está relacionada à classe de dispositivo USB.

> Os leitores de cartão inteligente devem ser instalados com um driver de dispositivo correspondente no dispositivo do usuário.

Para obter informações sobre leitores de cartão inteligente suportados, consulte a documentação do aplicativo Citrix Workspace que você está usando. Na documentação do aplicativo Citrix Workspace, as versões suportadas são listadas em um artigo sobre cartão inteligente ou no artigo de requisitos do sistema.

Experiência do usuário

O suporte a smart card é integrado ao Citrix Virtual Apps and Desktops, usando um canal virtual de smart card ICA/HDX específico que é habilitado por padrão.

Importante: Não use o redirecionamento USB genérico para leitores de smart card. Isso é desabilitado por padrão para leitores de smart card e não é suportado se habilitado.

Vários smart cards e vários leitores podem ser usados no mesmo dispositivo do usuário, mas se a autenticação pass-through estiver em uso, apenas um smart card deve ser inserido quando o usuário inicia um desktop ou aplicativo virtual. Quando um smart card é usado dentro de um aplicativo (por exemplo, para funções de assinatura digital ou criptografia), pode haver outros prompts para inserir um smart card ou digitar um PIN. Isso pode ocorrer se mais de um smart card tiver sido inserido ao mesmo tempo.

- Se os usuários forem solicitados a inserir um smart card quando o smart card já estiver no leitor, eles deverão selecionar Cancelar.
- Se os usuários forem solicitados a digitar o PIN, eles deverão digitá-lo novamente.

Você pode redefinir PINs usando um sistema de gerenciamento de cartão ou utilitário do fornecedor.

> **Importante:**

> Dentro de uma sessão do Citrix Virtual Apps ou Citrix Virtual Desktops, o uso de um smart card com o aplicativo Microsoft Remote Desktop Connection não é suportado. Isso às vezes é descrito como um uso de "salto duplo".

Antes de implantar smart cards

- Obtenha um driver de dispositivo para o leitor de smart card e instale-o no dispositivo do usuário. Muitos leitores de smart card podem usar o driver de dispositivo CCID fornecido pela Microsoft.
- Obtenha um driver de dispositivo e software de provedor de serviços criptográficos (CSP) do seu fornecedor de smart card e instale-os em dispositivos de usuário e desktops virtuais. O driver e o software CSP devem ser compatíveis com o Citrix Virtual Apps and Desktops; verifique a documentação do fornecedor para compatibilidade. Para desktops virtuais que usam smart cards que suportam e usam o modelo de minidriver, os minidrivers de smart card são baixados automaticamente, mas você também pode obtê-los em http://catalog.update.microsoft.com ou do seu fornecedor. Além disso, se o middleware PKCS#11 for necessário, obtenha-o do fornecedor do cartão.
- Importante: A Citrix recomenda que você instale e teste os drivers e o software CSP em um computador físico antes de instalar o software Citrix.
- Adicione a URL do Citrix Receiver™ for Web à lista de Sites Confiáveis para usuários que usam smart cards no Internet Explorer com Windows 10. No Windows 10, o Internet Explorer não é executado no modo protegido por padrão para sites confiáveis.
- Certifique-se de que sua infraestrutura de chave pública (PKI) esteja configurada adequadamente. Isso inclui garantir que o mapeamento de certificado para conta esteja configurado corretamente para o ambiente do Active Directory e que a validação do certificado do usuário possa ser realizada com sucesso.
- Certifique-se de que sua implantação atenda aos requisitos de sistema dos outros componentes Citrix usados com smart cards, incluindo o aplicativo Citrix Workspace e o StoreFront.
- Garanta o acesso aos seguintes servidores em seu Site:
  - O controlador de domínio do Active Directory para a conta de usuário 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 usuários para Acesso Remoto ao PC.

Etapa 3. Instale e configure o Delivery Controller e o StoreFront (se ainda não estiverem instalados) para o redirecionamento 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 de 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 redirecionamento de cartão inteligente, habilitando a comunicação de dados do cartão inteligente entre o aplicativo Citrix Workspace em um dispositivo de usuário e uma sessão de desktop virtual.

Etapa 7. Habilite os dispositivos de usuário (incluindo máquinas ingressadas ou não ingressadas no domínio) para o uso de cartão inteligente. Consulte 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 de cartão inteligente.

Etapa 8. Teste a implantação. Certifique-se de que a implantação esteja configurada corretamente iniciando um desktop virtual com o cartão inteligente de um usuário de teste. Teste todos os mecanismos de acesso possíveis (por exemplo, acessando o desktop através do Internet Explorer e do aplicativo Citrix Workspace).

Rastrear contagem de inserções do leitor de cartão inteligente

Com o acesso remoto de cartão inteligente, você pode rastrear o número de vezes que um cartão inteligente foi inserido ou removido de um leitor usando a função SCardGetStatusChange. A função atualiza um array de estruturas de dados SCARD_READERSTATE — uma para cada leitor que você monitora. A palavra alta (16 bits) do campo dwEventState de cada SCARD_READERSTATE contém a contagem do leitor. Para obter mais informações, consulte os artigos da Microsoft SCardGetStatusChangeA function e SCARD_READERSTATEA structure.

A configuração **Relatório de Contagem de Inserções do Leitor** está desabilitada por padrão. Para habilitar o rastreamento, adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

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 STOREFRONT™
Computadores locais ingressados no domínio	Conectado diretamente
Acesso remoto de computadores ingressados no domínio	Conectado através do Citrix Gateway
Computadores não ingressados no domínio	Conectado diretamente
Acesso remoto de computadores não ingressados no domínio	Conectado através do Citrix Gateway

TIPO	CONECTIVIDADE STOREFRONT™
Computadores não ingressados no domínio e thin clients acessando o site do Desktop Appliance	Conectado através de sites do Desktop Appliance
Computadores ingressados no domínio e thin clients acessando o StoreFront através da URL dos Serviços XenApp®	Conectado através de 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 dentro de uma única floresta. Logons de cartão inteligente entre florestas exigem uma confiança de floresta bidirecional direta para todas as contas de usuário. Implantações multifloresta mais complexas envolvendo cartões inteligentes (ou seja, onde as confianças são apenas unidirecionais ou de tipos diferentes) não são suportadas.

Você pode usar cartões inteligentes em um ambiente Citrix que inclui desktops remotos. Esse recurso pode ser instalado localmente (no dispositivo do usuário ao qual o cartão inteligente está conectado) ou remotamente (no desktop remoto ao qual o dispositivo do usuário se conecta).

Política de remoção de cartão inteligente

A política de remoção de cartão inteligente definida no produto determina o que acontece se você remover o cartão inteligente do leitor durante uma sessão. A política de remoção de cartão inteligente é configurada e gerenciada pelo sistema operacional Windows.

CONFIGURAÇÃO DA POLÍTICA	COMPORTAMENTO DA ÁREA DE TRABALHO
Nenhuma ação	Nenhuma ação.
Bloquear estação de trabalho	A sessão da área de trabalho é desconectada e a área de trabalho virtual é bloqueada.
Forçar logoff	O usuário é forçado a fazer logoff. Se a conexão de rede for perdida e essa configuração estiver ativada, a sessão poderá ser desconectada e o usuário poderá perder dados.
Desconectar se for uma sessão remota do Terminal Services	A sessão é desconectada e a área de trabalho virtual é bloqueada.

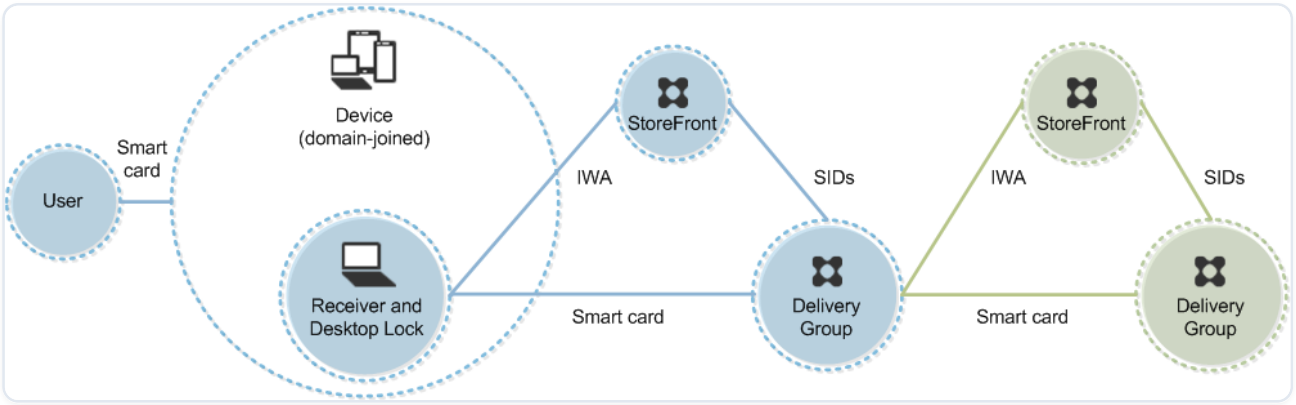
Verificação de revogação de certificado

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

Essa implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.

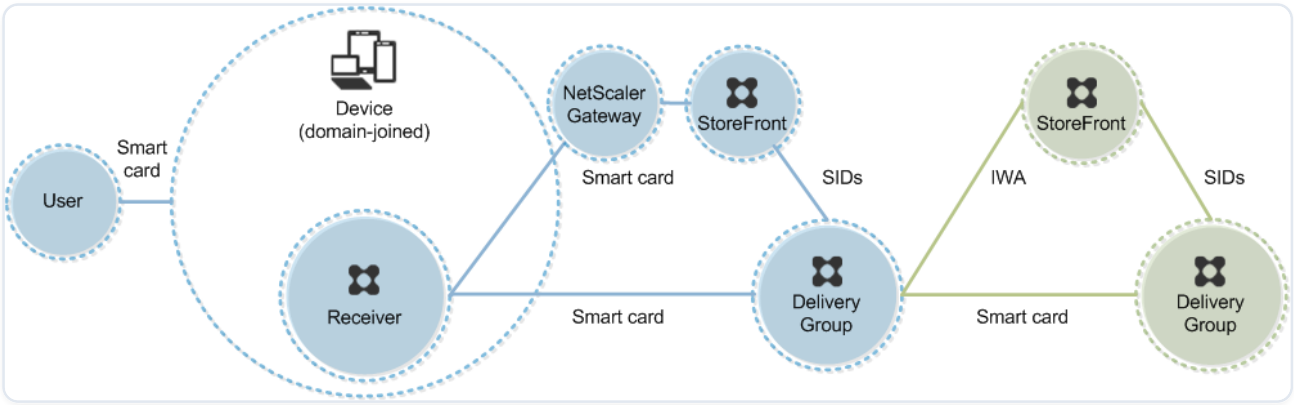


Um usuário faz logon em um dispositivo usando um cartão inteligente e um PIN. O Receiver autentica o usuário em um servidor StoreFront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. 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

Essa implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam ao StoreFront através do Citrix Gateway/Access Gateway.



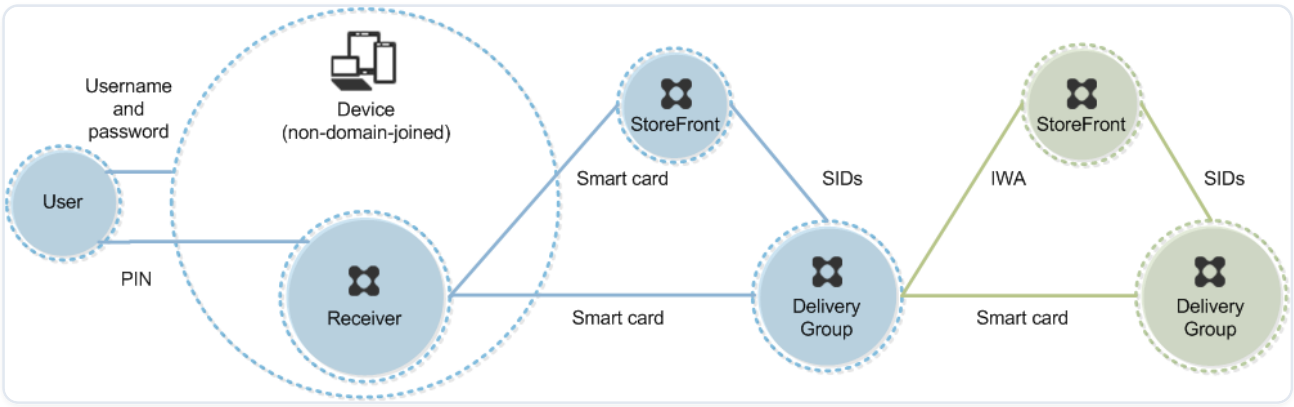
Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN, e então faz logon novamente no Citrix Gateway/Access Gateway. Este segundo logon pode ser com o cartão inteligente e PIN ou com um nome de usuário e senha, pois o Receiver permite autenticação bimodal nesta implantação.

O usuário é automaticamente conectado ao StoreFront, que passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps™ ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual ou aplicativo, o usuário não é solicitado novamente por 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

Essa 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

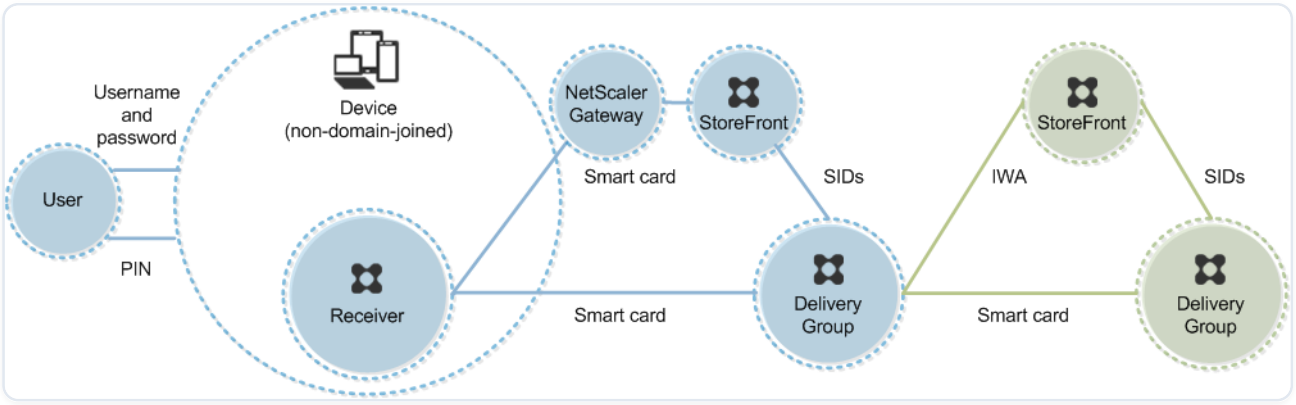
solicita ao usuário um cartão inteligente e PIN ou um nome de usuário e senha. O Receiver então autentica-se no Storefront.

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, o usuário é solicitado novamente por 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 ao 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 virtual ou aplicativo, o usuário é solicitado a inserir um PIN novamente porque o recurso de logon único não está disponível nesta implantação.

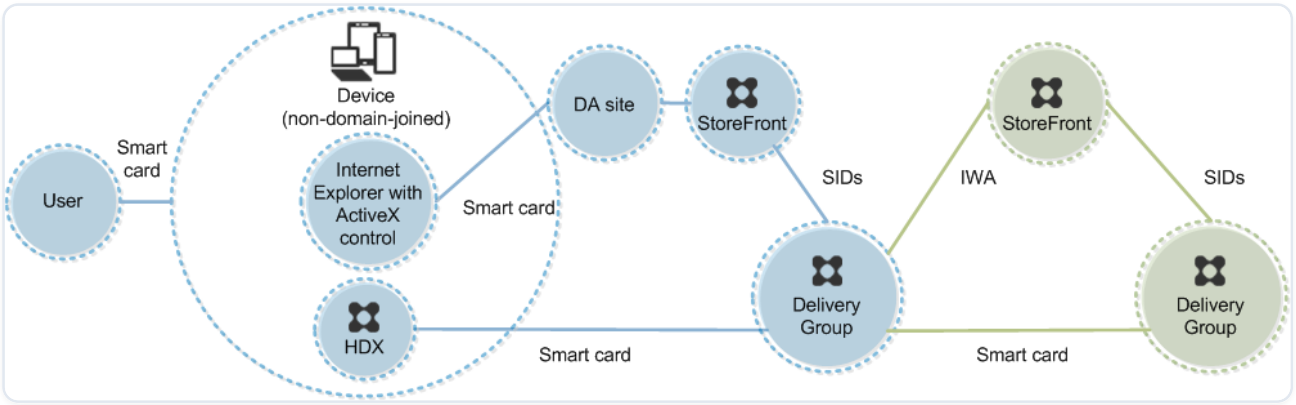
Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no

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.



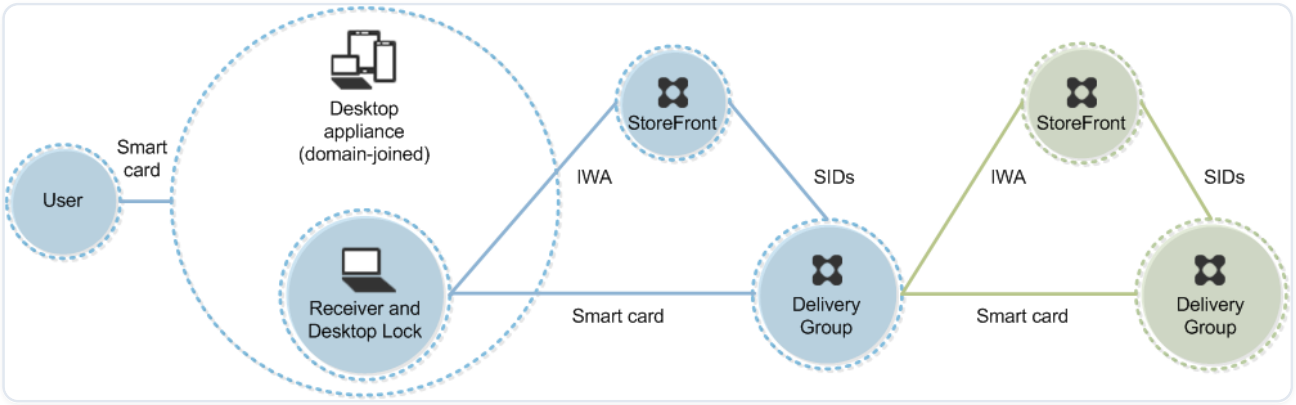
Um usuário faz logon em um dispositivo com um cartão inteligente. Se o Desktop Lock estiver em execução no dispositivo, o dispositivo será configurado para iniciar um site do Desktop Appliance por meio do Internet Explorer em execução no Modo Quiosque. Um controle ActiveX no site solicita ao usuário 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 desktop virtual e aplicativos. 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 configurar 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.

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 este recurso, consulte Redirecionamento FIDO2.

NOTA

Observe que este recurso não oferece suporte ao login na sessão virtual usando WebAuthn ou FIDO2. Este recurso permite apenas o uso desses métodos de autenticação em aplicativos dentro da sessão virtual.

> Este recurso não é 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	Compatível	Não compatível
Windows Server 2022	Compatível	Compatível
Windows 10	Compatível	Compatível
Windows 11	Compatível	Compatível

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

- Somente navegadores de 64 bits

Métodos de autenticação suportados

- Chave de Segurança FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial
    - Leitor de impressão digital
  - WebAuthn

Autenticação de aplicativo UWP

Com o lançamento do Citrix Virtual Apps and Desktops 2112, 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 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

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 em Controllers.

  Opcionalmente, você pode alterar as portas que o Controller usa para escutar o tráfego HTTP e HTTPS.

- Habilite as 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 manualmente em um VDA.
  - Configure o TLS nos Delivery Groups que contêm os VDAs executando um conjunto de cmdlets do 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 os componentes, criar um Site, criar catálogos de máquinas e criar Delivery Groups.
    - Para configurar o TLS nos Delivery Groups, você deve ter permissão para alterar as regras de acesso do Controller. Um Administrador Completo tem essa permissão.
    - Para configurar o TLS nos VDAs, você deve ser um administrador do Windows na máquina onde o VDA está instalado.
    - Em VDAs agrupados que são provisionados por Machine Creation Services™ ou Provisioning Services, a imagem da máquina VDA é redefinida na reinicialização,

fazendo com que as configurações TLS anteriores sejam perdidas. Execute o script PowerShell cada vez que o VDA for reiniciado para reconfigurar as configurações TLS.

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 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

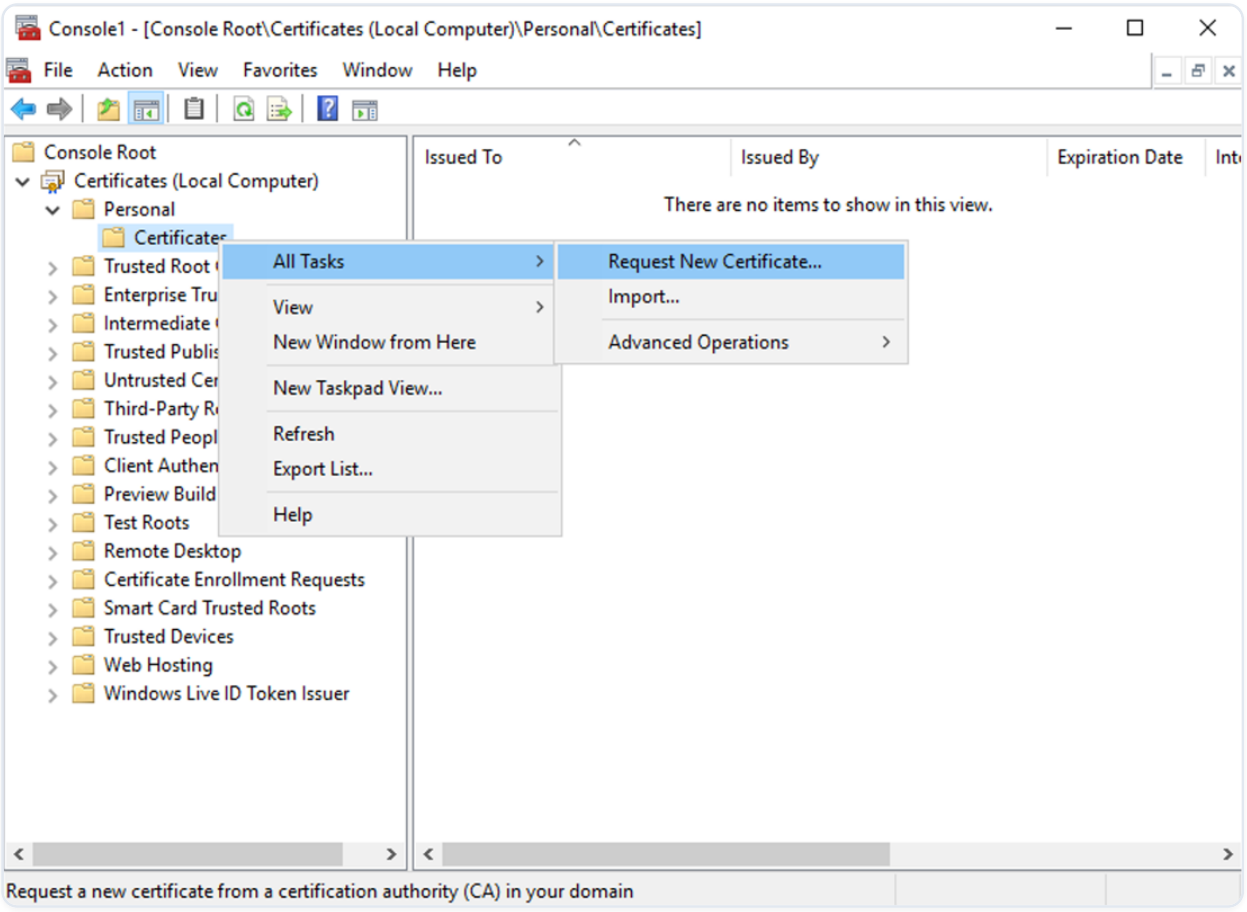
Para HTTPS, o Serviço XML oferece suporte a recursos TLS usando certificados de servidor, não certificados de cliente. Esta seção descreve a aquisição e instalação de certificados TLS em Delivery Controllers. As mesmas etapas podem ser aplicadas a Cloud Connectors para criptografar o tráfego STA e XML.

Embora existam vários tipos diferentes de autoridades de certificação e métodos de solicitação de certificado, 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.

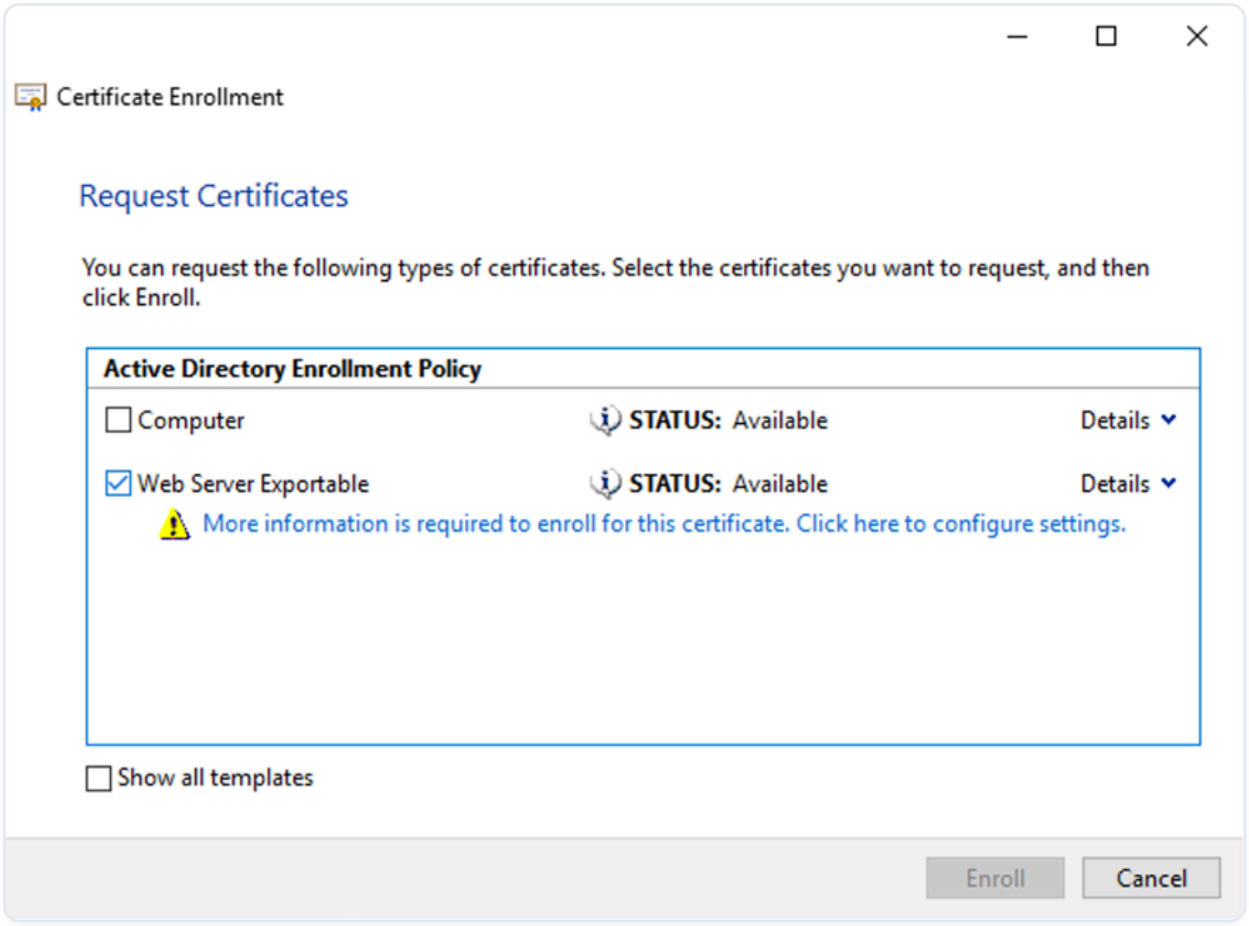
Se a Autoridade de Certificação da Microsoft estiver integrada a um domínio do Active Directory ou à floresta confiável à qual os Delivery Controllers estão unidos, você poderá adquirir um certificado do assistente de Registro de Certificado do snap-in Certificados do MMC.

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 de menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.



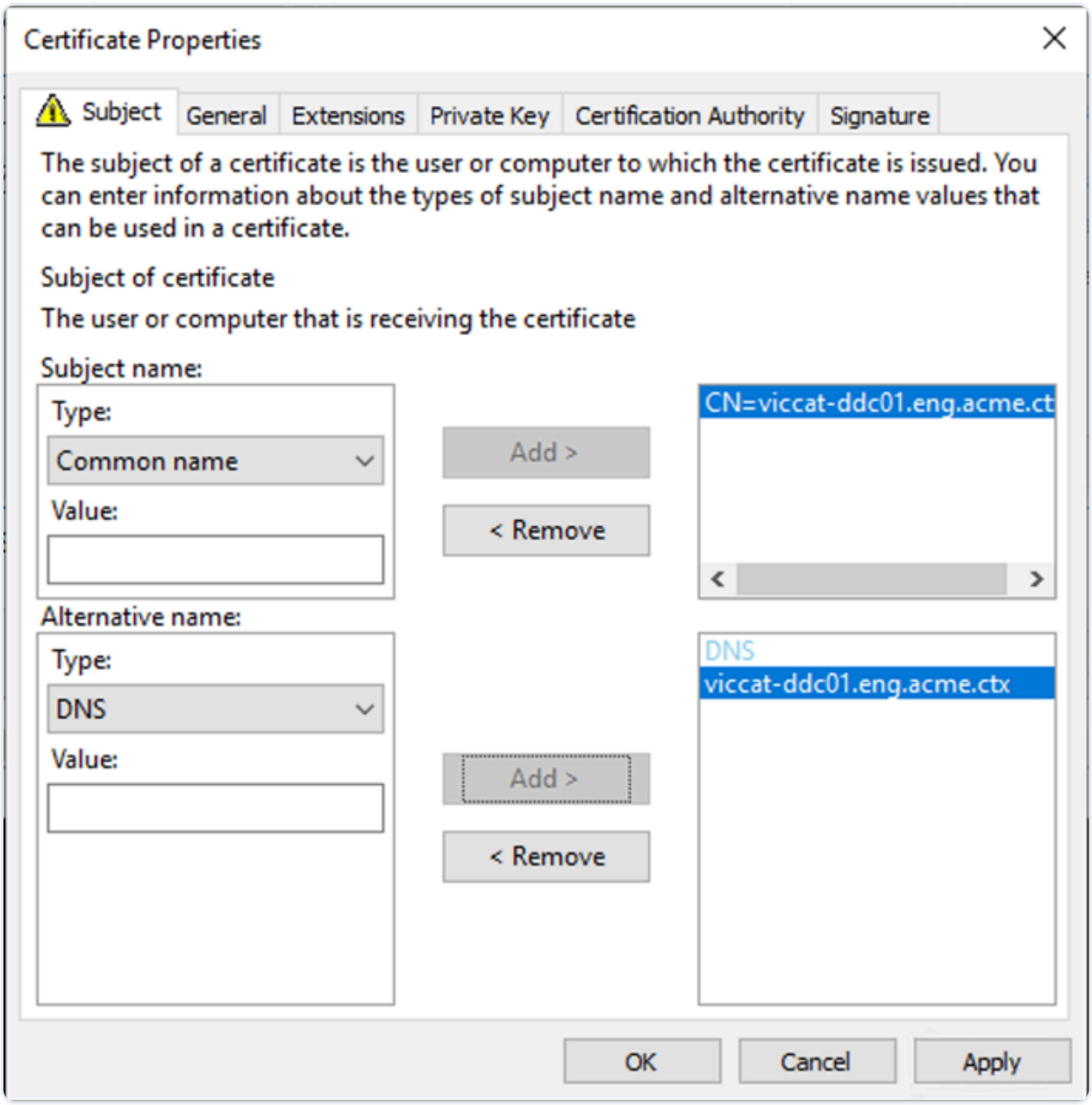
3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.
4. Selecione o modelo para o certificado de Autenticação de Servidor. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, 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 ouvinte SSL/TLS

Se o componente IIS do Windows estiver instalado no mesmo servidor, que é instalado como parte do Web Studio e do Director, você pode configurar o TLS usando o IIS. Para obter mais informações, consulte Habilitar TLS no Web Studio e no Director. Caso contrário, para configurar o certificado usando o PowerShell:

1. Para verificar se há um certificado existente vinculado, abra um prompt de comando e execute `netsh http show sslcert`:

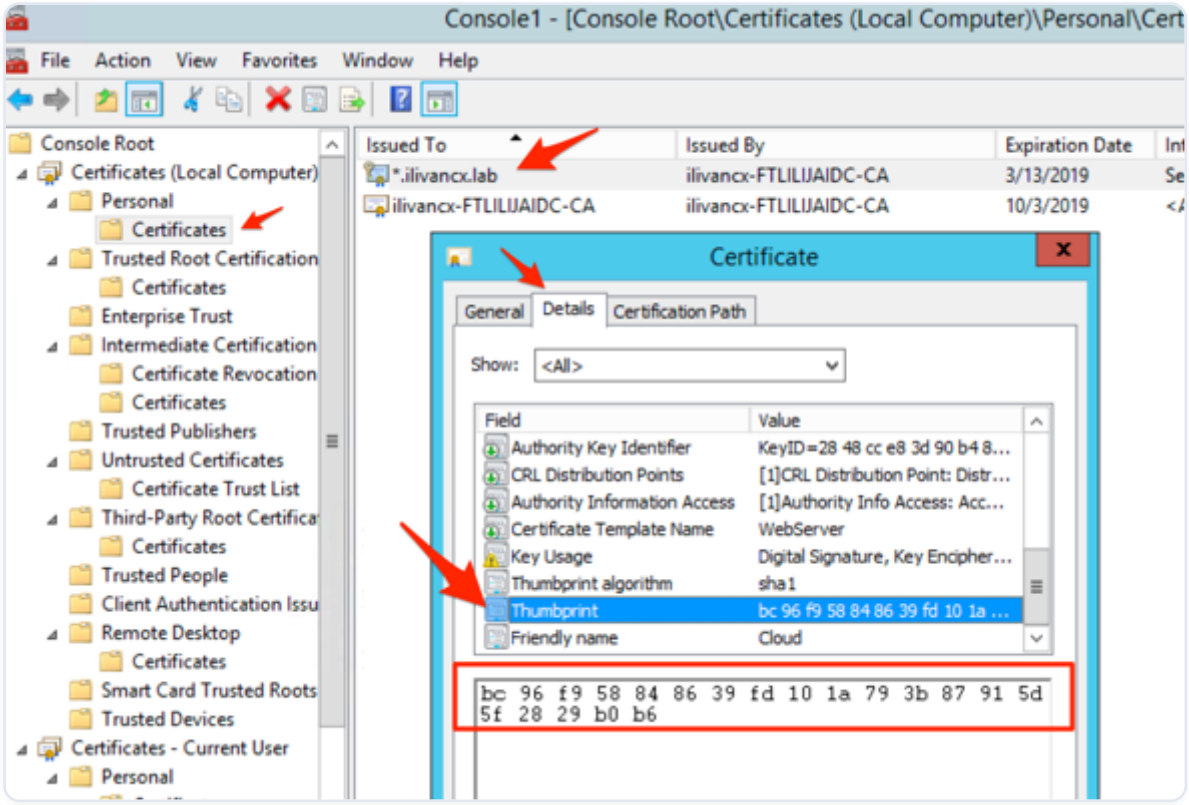
   ```
   netsh http show sslcert
   ```

2. Se houver uma vinculação existente, exclua-a.

```
netsh http delete sslcert ipport=0.0.0.0:443
```

Substituindo `0.0.0.0:443` por um endereço IP e porta específicos, se houver um especificado na vinculação existente.

3. Encontre a impressão digital do certificado que você instalou anteriormente. Para visualizar a impressão digital, abra **Gerenciar certificados do computador**, navegue até o certificado, abra-o e vá para a guia **Detalhes**.



Alternativamente, você pode usar o PowerShell. Por exemplo, o script a seguir procura um certificado cujo nome comum corresponde ao nome do host do servidor e imprime a impressão digital:

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

Se o nome comum do certificado não corresponder aos nomes de host, isso falhará. Se houver vários certificados para o nome do host, isso retornará várias impressões digitais concatenadas e você deverá escolher a impressão digital apropriada.

O exemplo a seguir procura um certificado pelo nome amigável:

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

Se houver vários certificados com o nome amigável especificado, isso retornará várias impressões digitais concatenadas e você deverá escolher a impressão digital apropriada.

4. Para vincular o certificado à porta, use o comando `netsh http add sslcert`:

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: O endereço IP e a porta. Usar 0.0.0.0:443 aplica isso a todos os endereços IP. Você pode, em vez disso, especificar um endereço IP específico.
- `certhash`: A impressão digital do certificado que você identificou na etapa anterior.
- `appid`: O GUID do Serviço de Agente Citrix.

> **Observação:**
>
> Ao renovar um certificado ou refazer a vinculação, use o `appid` específico associado ao Serviço de Broker em vez de um GUID arbitrário.
>
> Para encontrar o `appid` correto para o Citrix Broker Service:

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 Citrix Broker Service na saída (por exemplo, `{D333C884-187F-447C-8C67-463F33989C8F}`). Use este GUID para o parâmetro `appid`.

- `disablelegacytls=enable`: Desativa versões legadas de TLS. Este parâmetro está disponível no Windows 2022 e superior. No Windows 2022, ele desativa TLS 1.0 e 1.1. No Windows 2025, isso é desnecessário, pois TLS 1.0 e 1.1 são desativados por padrão.

Por exemplo, execute o seguinte comando para vincular o certificado com a impressão digital `bc96f958848639fd101a793b87915d5f2829b0b6` à porta `443` em todos os endereços IP:

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

Uma vez que o HTTPS esteja habilitado, você deve configurar quaisquer implantações do StoreFront e Netscaler Gateways para usar HTTPS em vez de HTTP para se conectar ao delivery controller.

Observação:

Se o Controller estiver instalado no Windows Server 2016 e o StoreFront estiver instalado no Windows Server 2012 R2, uma alteração de configuração será necessária no Controller para alterar a ordem das suites de cifras TLS. Esta 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 estas 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 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 Microsoft MSDN, 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 de 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. Essa configuração é feita para você quando você usa o script do 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 e TLS 1.2. Especifique a versão mínima permitida; todas as conexões de protocolo que usam 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 1.2 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 1.2 como a versão mínima, somente as conexões TLS 1.2 serão permitidas.

DTLS 1.0 corresponde a TLS 1.1, e DTLS 1.2 corresponde a TLS 1.2.

- **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 (Citrix Workspace app 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(ernamental), 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
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X

CONJUNTO DE CIFRAS TLS/ DTLS	TODOS	COM	GOV	TODOS	COM	GOV
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

* Não compatível com o Windows Server 2012 R2.

Nota:

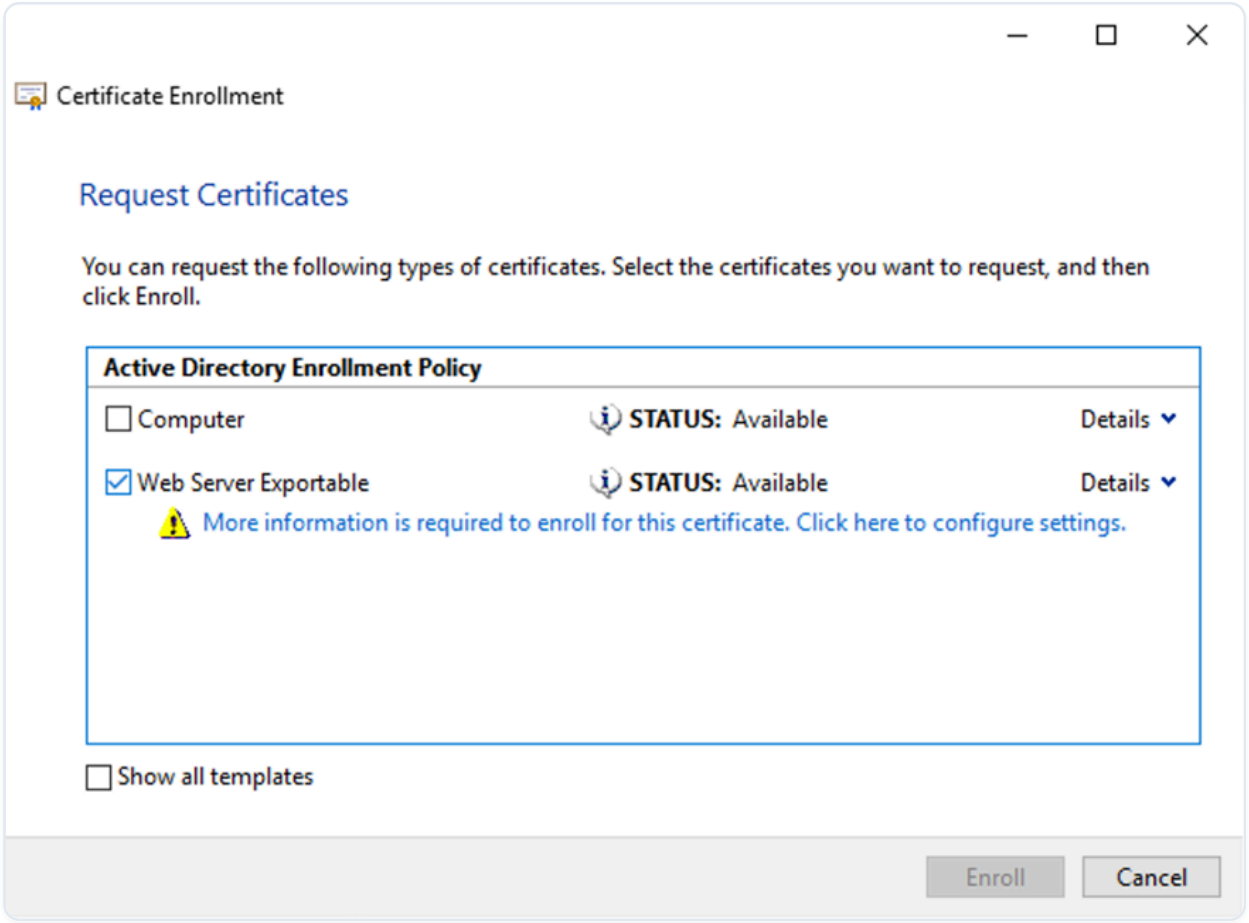
O VDA não suporta conjuntos de cifras DHE (por exemplo, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 e TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Se selecionados pelo Windows, eles podem não ser usados pelo Receiver.

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**, então 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.

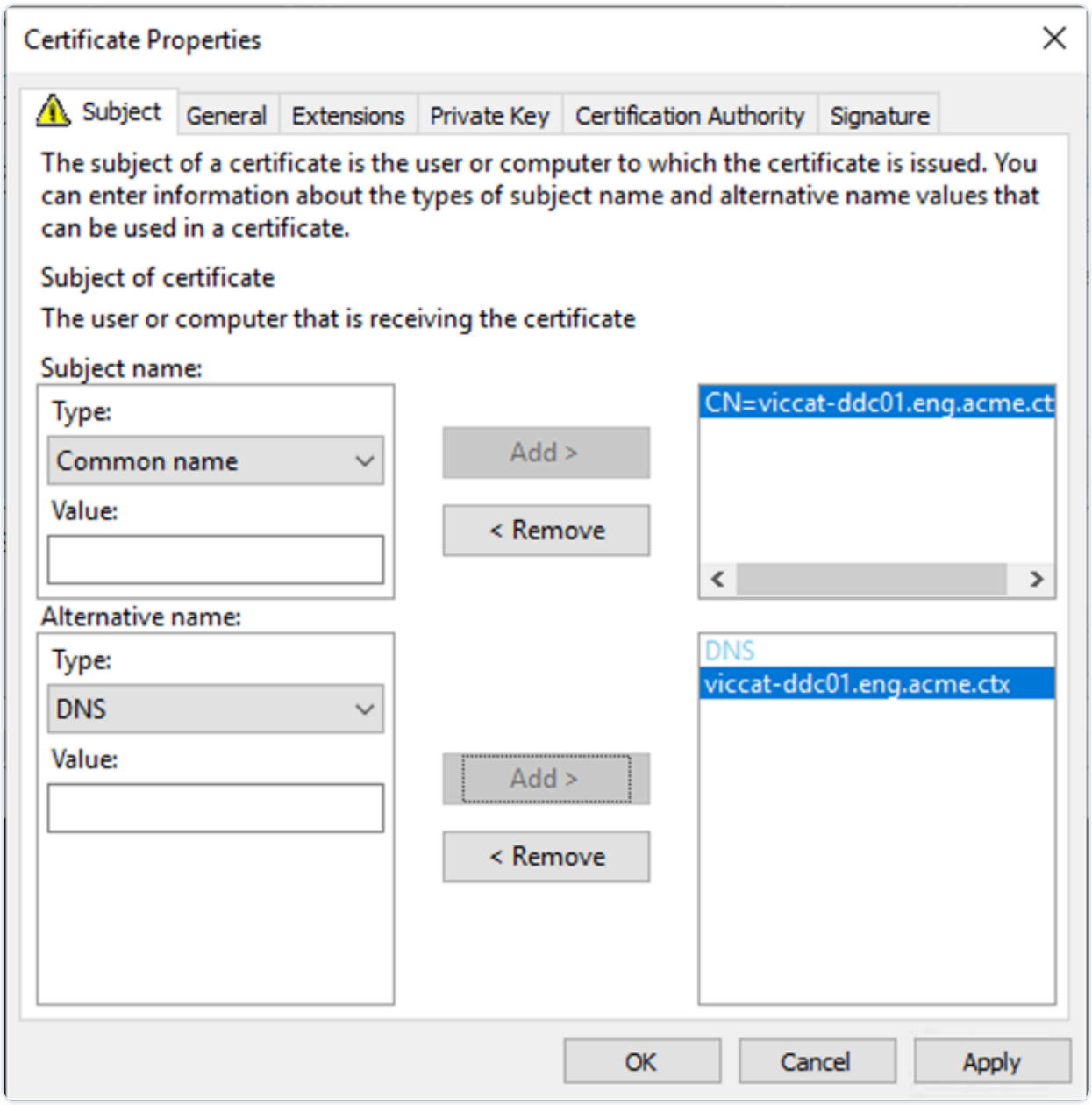
4. Selecione o modelo para o certificado de Autenticação de Servidor. Ambos os padrões do Windows **Computer** ou **Web Server Exportable** são aceitáveis. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você pode clicar em **Registrar** sem fornecer mais detalhes.



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



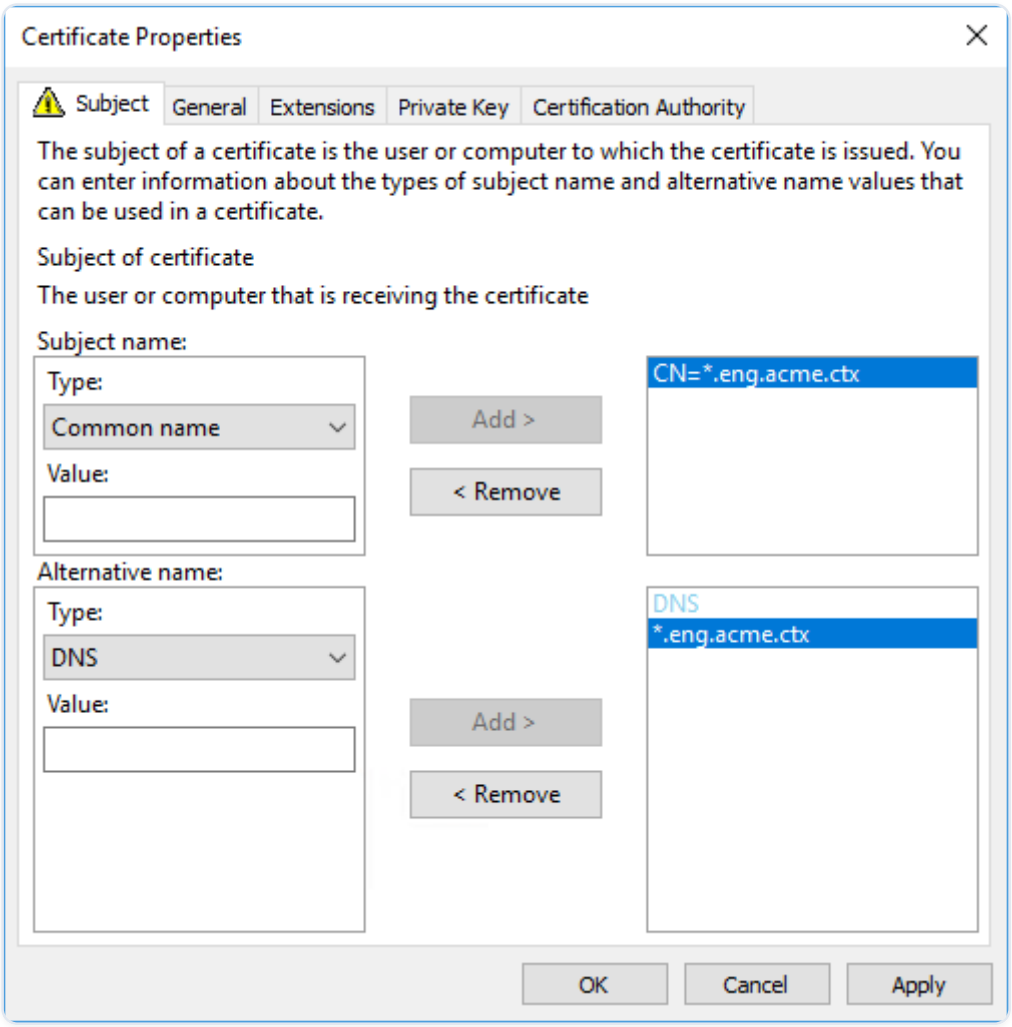
Nota:

Use o Registro Automático de Certificados dos Serviços de Certificados do Active Directory para automatizar a emissão e a implantação de certificados nos VDAs. Isso é descrito em `<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

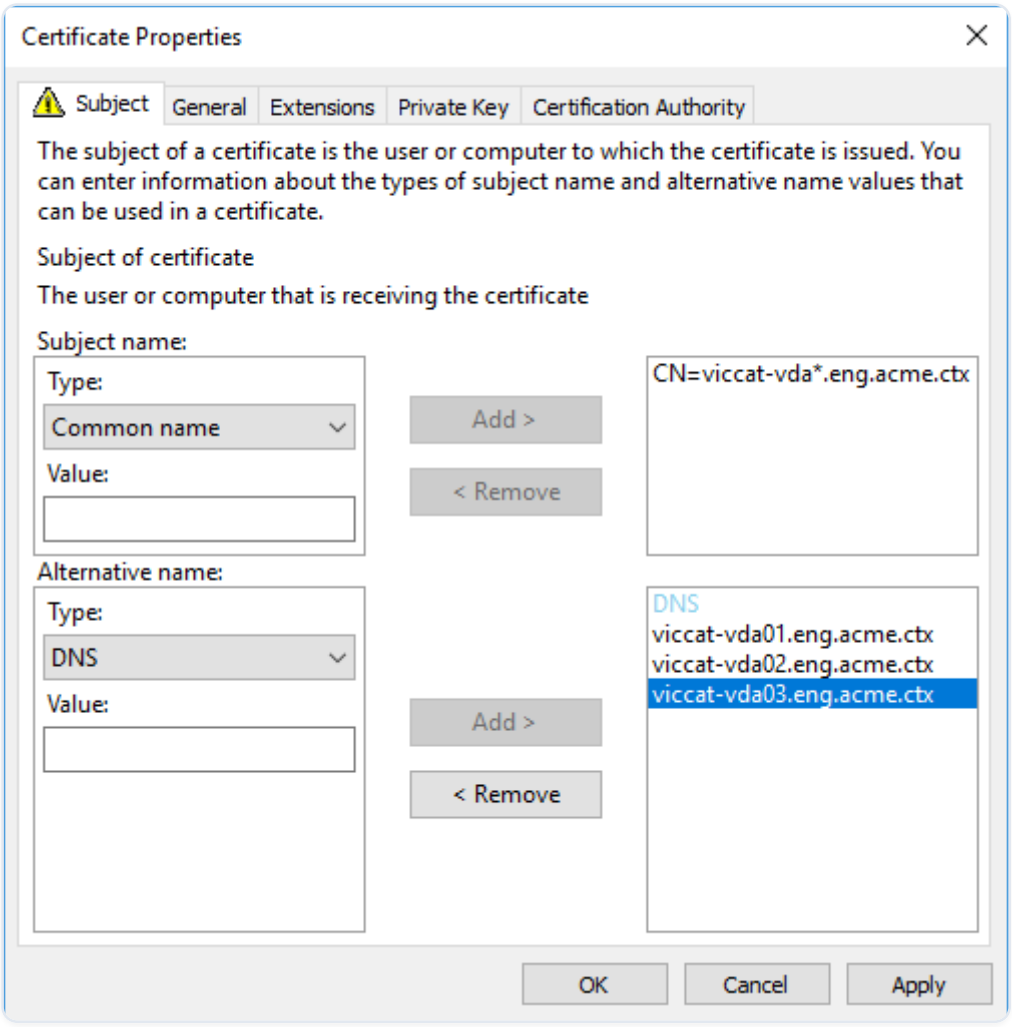
Nome alternativo — selecione o tipo **DNS** e adicione o *.primary.domain dos VDAs



Você pode usar certificados SAN para permitir que um único certificado proteja vários VDAs específicos:

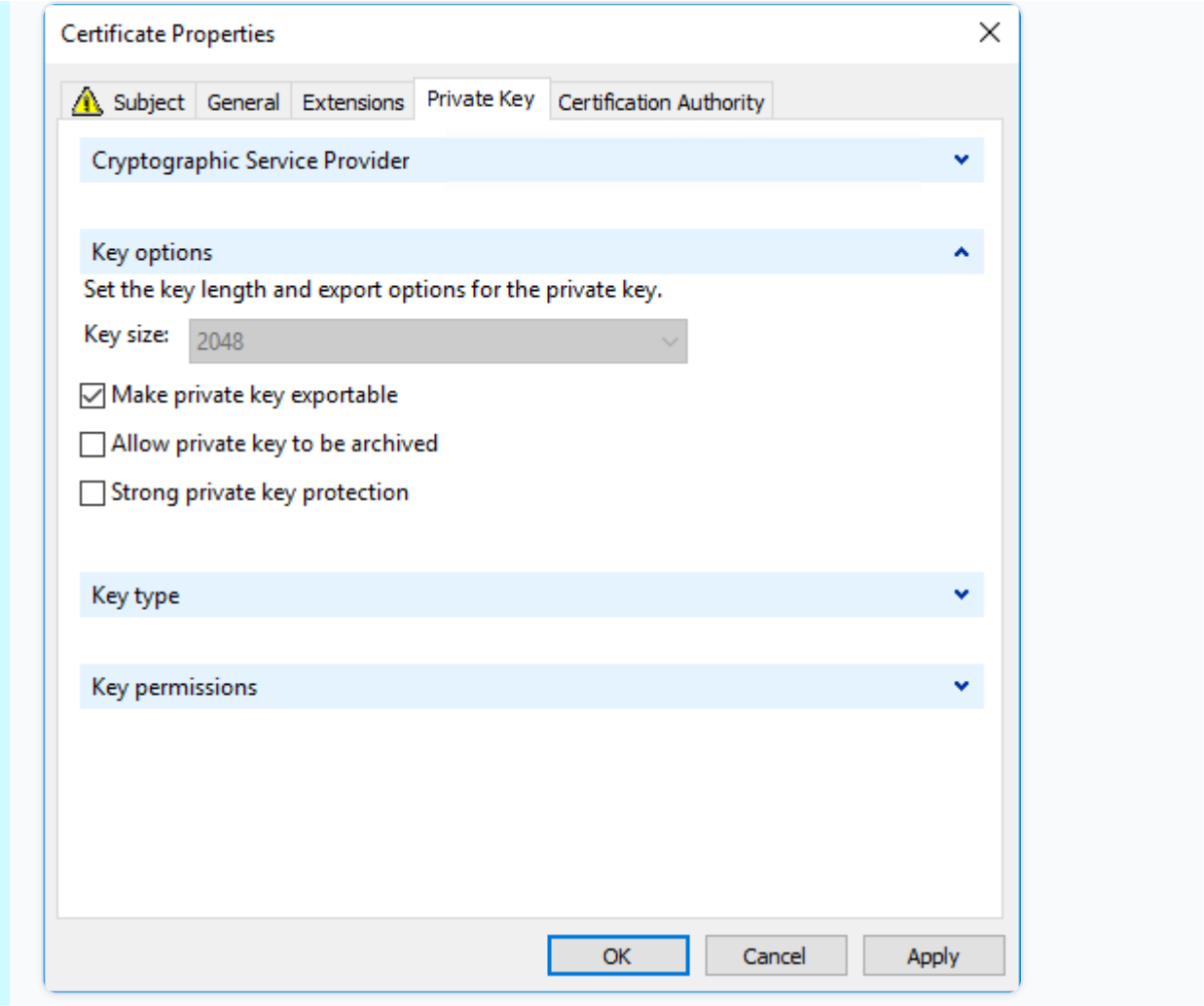
Nome do assunto — selecione o tipo **Nome comum** e insira uma string para ajudar a identificar o uso do certificado

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 uma negociação TLS ideal.



Nota:

Tanto os certificados curinga quanto os SAN exigem que **Tornar a chave privada exportável** na guia Chave Privada seja selecionado:



Configurar TLS em um VDA usando o script PowerShell

Instale o Certificado TLS na área Local Computer > Personal > Certificates do armazenamento de certificados. Se mais de um certificado residir nesse local, forneça a impressão digital do certificado ao script PowerShell.

Nota:

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 a impressão digital quando apenas um único certificado está presente para o FQDN do VDA.

O script Enable-VdaSSL.ps1 habilita ou desabilita o ouvinte TLS em um VDA. Este script está disponível na pasta *Support* > *Tools* > *SslSupport* na mídia de instalação.

Quando você habilita o TLS, os conjuntos de cifras DHE são desativados. Os conjuntos de cifras ECDHE não são afetados.

Quando você habilita o TLS, o script desativa 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 desativa 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.

> **Nota:**
>
> DTLS não é suportado com Áudio ICA/HDX sobre Transporte UDP em Tempo Real, ou com ICA/HDX Framehawk.

> Consulte Portas de rede.

O script contém as seguintes descrições de sintaxe, além de exemplos adicionais; 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 listener TLS no VDA. Este parâmetro ou o parâmetro Disable é obrigatório.

PARÂMETRO	DESCRIÇÃO
Disable	Desabilita o listener TLS no VDA. Este parâmetro ou o parâmetro Enable é obrigatório. Se você especificar este parâmetro, nenhum outro parâmetro será válido.
CertificateThumbPrint "<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.
SSLPort <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_1.2”.
SSLCipherSuite "<conjunto>"	Conjunto de cifras TLS, entre aspas. Valores válidos: "GOV", "COM" e "ALL" (padrão).

Exemplos

O script a seguir instala e habilita o valor da versão do protocolo TLS. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

O script a seguir instala e habilita o ouvinte TLS e especifica a porta TLS 400, o conjunto de cifras GOV e um valor mínimo de protocolo TLS 1.2. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"
```

```
-SSLCipherSuite "All"
```

O script a seguir desabilita o ouvinte TLS no VDA.

```
Enable-VdaSSL -Disable
```

Configurar o TLS manualmente em um VDA

Ao configurar o TLS em um VDA manualmente, você concede acesso de leitura genérico à chave privada do certificado TLS para o serviço apropriado em cada VDA: NT SERVICE\PorticaService para um VDA para SO de sessão única do Windows, ou NT SERVICE\TermService para um VDA para SO de múltiplas sessões do Windows. Na máquina onde o VDA está instalado:

ETAPA 1. Inicie o console de gerenciamento da Microsoft (MMC): Iniciar > Executar > mmc.exe.

ETAPA 2. Adicione o snap-in Certificados ao MMC:

1. Selecione Arquivo > Adicionar/Remover Snap-in.
2. Selecione Certificados e clique em Adicionar.
3. Quando solicitado com "Este snap-in sempre gerenciará certificados para:", escolha "Conta de computador" e clique em Avançar.
4. Quando solicitado com "Selecione o computador que você deseja que este snap-in gerencie", escolha "Computador local" e clique em Concluir.

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 SO Windows multissessão, "TERMSERVICE"

ETAPA 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 1.2. 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 SO Windows multissessão, reinicie a máquina para que as alterações entrem em vigor. (Você não precisa reiniciar máquinas que contêm VDAs para SO Windows de sessão única.)

> **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
```

Observação:

Os seis primeiros 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 (Citrix Workspace app ou StoreFront).

Essa 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 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 Citrix Workspace app 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 Citrix Workspace app, Citrix Gateway e o VDA. Algumas configurações que usam DTLS entre o Citrix Workspace app e o Citrix Gateway, e que usam DTLS entre o Citrix Gateway e o VDA, exigem ação adicional.

É necessária uma ação adicional 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 opções:

- 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.

Observação:

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.

Redirecionamento de vídeo TLS e HTML5 e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer

uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX em execução no VDA. Para conseguir isso, o Serviço de Redirecionamento de Vídeo HTML5 gera dois certificados personalizados no armazenamento de certificados no VDA. 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.

Segurança da Camada de Transporte (TLS) no Servidor de Impressão Universal

O protocolo Transport Layer Security (TLS) é compatível com 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 — editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Tipos de conexões de impressão entre o VDA e o Servidor de Impressão Universal

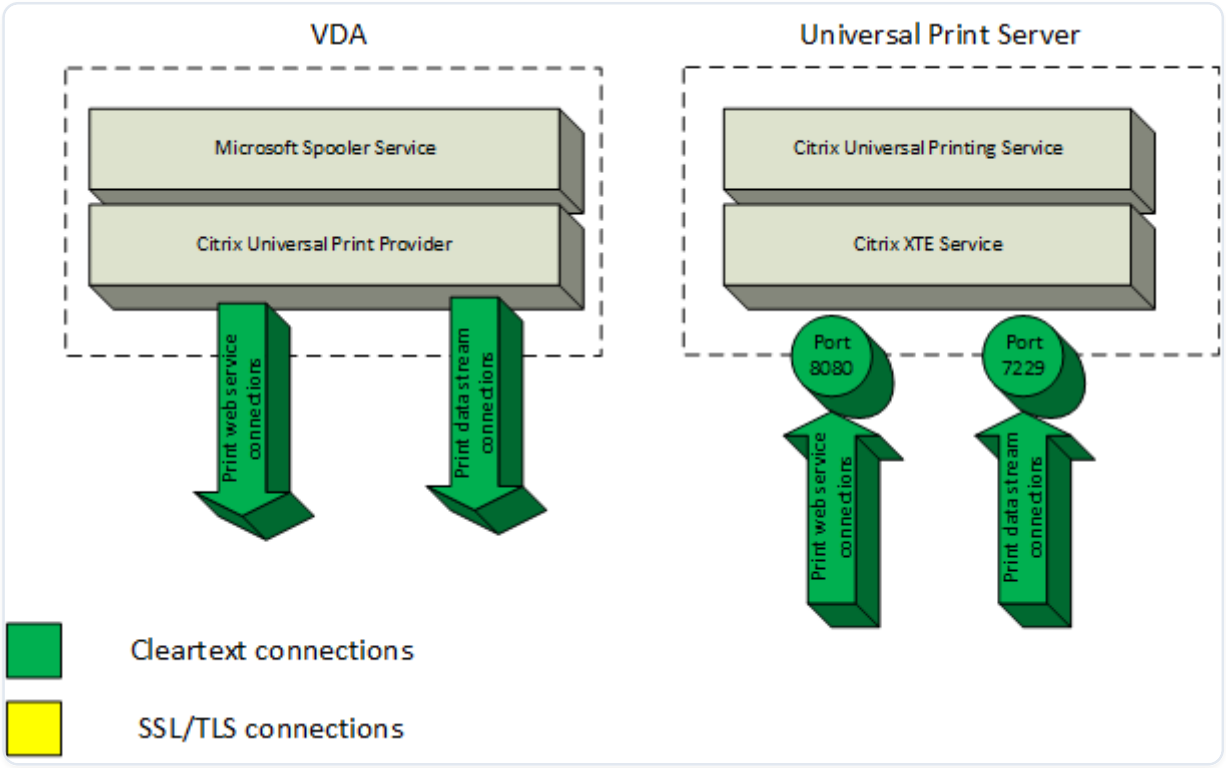
Conexões de texto não criptografado

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

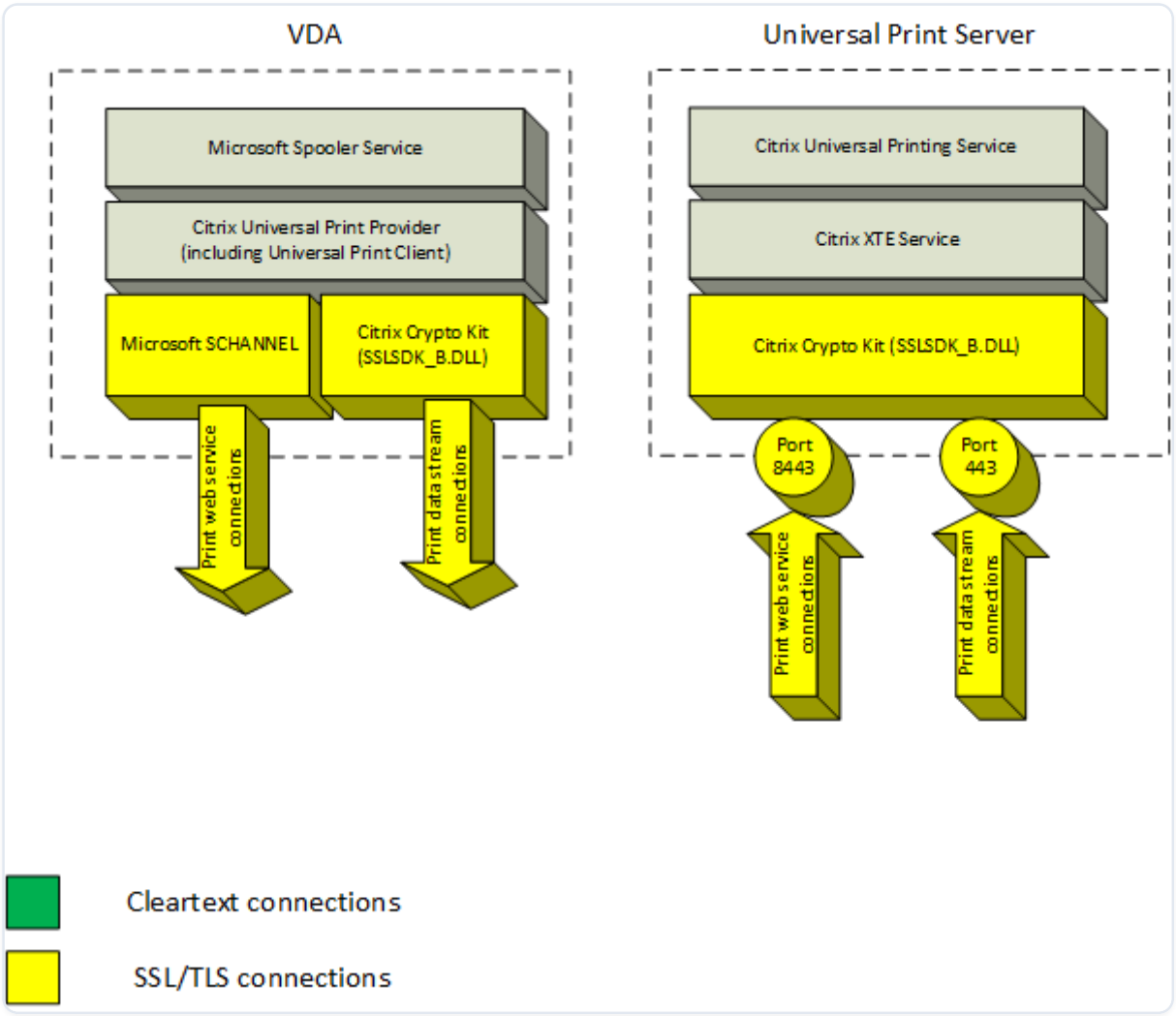
configurações de SSL/TLS neste documento não se aplicam às conexões NETBIOS e RPC feitas pelo serviço de Spooler de Impressão do Windows. O VDA usa o Provedor de Impressão de Rede do Windows (win32spl.dll) como um fallback se a configuração de política **Universal Print Server enable** estiver definida 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 TLS Registry Settings descreve as configurações de registro para o Microsoft SCHANNEL SSP.

Usando o Editor de Política de Grupo no VDA (Windows Server 2016 ou Windows 10), vá para **Configuração do Computador > 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

Observação:

Quando essa 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)

Essa 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 SSL/TLS para conexões de fluxo de dados de impressão criptografados (CGP) (porta TCP 443).

Configuração do servidor SSL/TLS

O Universal Print Server funciona como o servidor SSL/TLS.

Use o script PowerShell `Enable-UpsSsl.ps1` para configurar as configurações SSL/TLS.

Instalar o certificado do servidor TLS no Universal Print Server

Para HTTPS, o Universal Print Server oferece suporte a recursos TLS usando certificados de servidor. Certificados de cliente não são usados. Use os Serviços de Certificados do Microsoft

Active Directory ou outra autoridade de certificação para solicitar um certificado para o Universal Print Server.

Tenha em mente as seguintes considerações ao registrar/solicitar um certificado usando os Serviços de Certificados do Microsoft Active Directory:

1. Coloque o certificado no armazenamento de certificados **Pessoal** do Computador Local.
2. Defina o atributo **Nome Comum** do Nome Distinto do Assunto (Subject DN) do certificado para o nome de domínio totalmente qualificado (FQDN) do Universal Print Server. Especifique isso no modelo de certificado.
3. Defina o Provedor de Serviços Criptográficos (CSP) usado para gerar a solicitação de certificado e a chave privada como **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Especifique isso no modelo de certificado.
4. Defina o Tamanho da Chave para pelo menos 2048 bits. Especifique isso no modelo de certificado.

Configurando SSL no Universal Print Server

O Serviço XTE no Universal Print Server escuta as conexões de entrada. Ele funciona como um servidor SSL quando o SSL está habilitado. As conexões de entrada são de dois tipos: conexões de serviço web de impressão, que contêm comandos de impressão, e conexões de fluxo de dados de impressão, que contêm trabalhos de impressão. O SSL pode ser habilitado nessas conexões. O SSL protege a confidencialidade e a integridade dessas conexões. Por padrão, o SSL está desabilitado.

O script PowerShell usado para configurar o SSL está na mídia de instalação e tem este nome de arquivo: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Configurando 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 não criptografado (HTTP): 8080
- Porta TCP do fluxo de dados de impressão em texto não criptografado (CGP): 7229
- Porta TCP do serviço web de impressão criptografado (HTTPS): 8443
- Porta TCP do fluxo de dados de impressão criptografado (CGP): 443

Para alterar as portas usadas pelo Serviço XTE no Universal Print Server, execute os seguintes comandos no PowerShell como administrador (consulte a seção posterior para obter notas sobre o uso do script PowerShell Enable-UpsSsl.ps1):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` ou `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

Configurações de TLS no Universal Print Server

Se você tiver vários Universal Print Servers em uma configuração com balanceamento de carga, certifique-se de que as configurações de TLS estejam configuradas de forma consistente em todos os Universal Print Servers.

Ao configurar o TLS no Universal Print Server, as permissões no certificado TLS instalado são alteradas, concedendo ao Serviço de Impressão Universal acesso de leitura à chave privada do certificado e informando ao Serviço de Impressão Universal o seguinte:

- Qual certificado no armazenamento de certificados usar para TLS.
- Quais números de porta TCP usar para conexões TLS.

O Firewall do Windows (se ativado) deve ser configurado para permitir conexões de entrada nessas portas TCP. Essa configuração é feita automaticamente quando você usa o script PowerShell Enable-UpsSsl.ps1.

- Quais versões do protocolo TLS permitir.

O Universal Print Server suporta as versões 1.2, 1.1 e 1.0 do protocolo TLS. Especifique a versão mínima permitida.

A versão padrão do protocolo TLS é 1.2.

- Quais conjuntos de cifras TLS permitir.

Um conjunto de cifras seleciona os algoritmos criptográficos usados para uma conexão. VDAs e Universal Print Server podem suportar diferentes conjuntos de cifras. Quando um VDA se conecta e envia uma lista de conjuntos de cifras TLS suportados, o Universal Print Server compara um dos conjuntos de cifras do cliente com um dos conjuntos de cifras em sua própria lista de conjuntos de cifras configurados e aceita a conexão. Se não houver um conjunto de cifras correspondente, o Universal Print Server rejeita a conexão.

O Universal Print Server suporta os seguintes conjuntos de cifras nomeados GOV(ernamental), COM(ercial) e ALL para os modos OPEN, FIPS e SP800-52 nativos do Crypto Kit. 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_ECDHE_RSA_AES256_CBC_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_SHA									

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 **Suporte > Ferramentas > SslSupport** na mídia de instalação.

Quando você habilita o TLS, o script desabilita todas as regras existentes do Firewall do Windows para as portas TCP do Universal Print Server. Em seguida, ele adiciona novas regras que permitem que o Serviço XTE aceite conexões de entrada apenas nas portas TCP e UDP TLS. Ele também desabilita as regras do Firewall do Windows para:

- Conexões de serviço web de impressão em texto simples (padrão: 8080)
- Conexões de fluxo de dados de impressão em texto simples (CGP) (padrão: 7229)

O efeito é que o VDA pode fazer essas conexões somente ao usar TLS.

> **Observação:**
>
> A habilitação do TLS não afeta as conexões RPC/SMB do Windows Print Spooler originadas do VDA e que vão para o 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&gt;] [-CGPPort
&lt;portnum&gt;]
```

PARÂMETRO	DESCRIÇÃO
Habilitar	Habilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Disable é obrigatório.

PARÂMETRO	DESCRIÇÃO
Desabilitar	Desabilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Enable é obrigatório.
CertificateThumbprint `"<thumbprint>"`	Impressão digital do certificado TLS no armazenamento de certificados Pessoal do Computador Local, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar.
HTTPPort `<port>`	Porta do serviço web de impressão em texto simples (HTTP/SOAP). Padrão: 8080
CGPPort `<port>`	Porta de fluxo de dados de impressão em texto simples (CGP). Padrão: 7229
HTTPSPort `<port>`	Porta do serviço web de impressão criptografado (HTTPS/SOAP). Padrão: 8443
CGPSSLPort `<port>`	Porta de fluxo de dados de impressão criptografado (CGP). Padrão: 443
SSLMinVersion `"<version>"`	Versão mínima do protocolo TLS, entre aspas. Valores válidos: “TLS_1.0”, “TLS_1.1” e “TLS_1.2”. Padrão: TLS_1.2.
SSLCipherSuite `“<name>”`	Nome do pacote de conjunto de cifras TLS, entre aspas. Valores válidos: “GOV”, “COM” e “ALL” (padrão).
FIPSMode `<Boolean>`	Habilita ou desabilita o modo FIPS 140 no Servidor XTE. Valores válidos: $true para 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 desativa o TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Configurando o modo FIPS

Habilitar o modo Padrões Federais de Processamento de Informações dos EUA (FIPS) 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 ativar/desativar o modo FIPS do Windows.

Ativando o modo FIPS no cliente

No Delivery Controller™, execute o Citrix Studio e defina a configuração da política Citrix **Modo FIPS SSL** como **Habilitado**. Habilite a política Citrix.

Faça isso em cada VDA:

1. Ative o modo FIPS do Windows.
2. Reinicie o VDA.

Ativando 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 Delivery Controller, execute o Citrix Studio e defina a configuração da política Citrix **Modo FIPS SSL** como **Desativado**. Habilite a política Citrix. Você também pode excluir a configuração da política Citrix **Modo FIPS SSL**.

Faça isso em cada VDA:

1. Desative o modo FIPS do Windows.
2. Reinicie o VDA.

Desativando o modo FIPS no servidor

Faça isso em cada Universal Print Server:

1. Desative o modo FIPS do Windows.
2. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $false`.
4. Reinicie o Universal Print Server.

Configurando a versão do protocolo SSL/TLS

A versão padrão do protocolo SSL/TLS é TLS 1.2. TLS 1.2 é a única versão de protocolo SSL/TLS recomendada 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.

Configurando a versão do protocolo SSL/TLS no servidor

Faça isso em cada Universal Print Server:

1. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
2. Execute o script `Enable-UpsSsl.ps1` com os parâmetros de versão `-Enable -SSLMinVersion`. Lembre-se de reverter para TLS 1.2 quando terminar os testes.
3. Reinicie o Universal Print Server.

Configurando a versão do protocolo SSL/TLS no cliente

Faça isso em cada VDA:

1. No Delivery Controller, defina a configuração de política **Versão do Protocolo SSL** para a versão de protocolo desejada e habilite a política.
2. O artigo de suporte da Microsoft TLS Registry Settings descreve as configurações de registro para Microsoft SCHANNEL SSP. Habilite o lado do cliente **TLS 1.0, TLS 1.1 ou TLS 1.2** usando as configurações de registro.

> **Importante:**

> Lembre-se de restaurar as configurações de registro para seus valores originais quando terminar os testes.

3. Reinicie o VDA.

Solução de problemas

Se ocorrer um erro de conexão, verifique o arquivo de log C:\Program Files (x86)\Citrix\XTE\logs\error.log no Universal Print Server.

A mensagem de erro **SSL handshake from client failed** aparece neste arquivo de log se o handshake SSL/TLS falhar. Tais falhas podem ocorrer se a versão do protocolo SSL/TLS no VDA e no Universal Print Server não corresponderem.

Use o FQDN do Universal Print Server nas seguintes configurações de política que contêm nomes de host do Universal Print Server:

- Impressoras de sessão
- Atribuições de impressora
- Universal Print Servers para balanceamento de carga

Certifique-se de que o relógio do sistema (data, hora e fuso horário) estejam corretos nos Servidores de Impressão Universal e nos VDAs.

Segurança do canal virtual

Por padrão, o recurso de lista de permissões de canal virtual está ativado. Como resultado, apenas canais virtuais Citrix® têm permissão para abrir em sessões de aplicativos e desktops virtuais. Se houver necessidade de usar canais virtuais personalizados, sejam desenvolvidos internamente ou de terceiros, estes precisam ser adicionados explicitamente à lista de permissões.

Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa:

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 da política de lista de permissões de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, eles podem ser adicionados separados por vírgulas.

> **Observação:**

> Após fazer alterações na política, reinicie o VDA para garantir que as alterações entrem em vigor.

> Usando os exemplos anteriores, você adicionaria o seguinte à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Se houver vários processos, você adicionaria o seguinte à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Considerações sobre canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, existem dois recursos que exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- HDX™ RealTime Optimization Pack para Skype for Business

Redirecionamento Multimídia

Esta informação é necessária 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

Esta informação é necessária para a entrada da lista de permissões:

- Nome do canal virtual: CTXRMEP
- Processo: Caminho para o executável do Skype for Business na 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`

Obtendo 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 fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, essas informações podem ser obtidas 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 no seguinte evento:
    - Em um VDA de sessão única, ID de evento 2004 da origem Picadd.
    - Em um VDA de várias sessões, ID de evento 16 da origem Rpm.
3. Faça logoff da sessão.
4. Adicione uma entrada na configuração da política de lista de permissões de canais virtuais para o canal virtual identificado, apenas com o nome do canal virtual.
5. Reinicie o VDA.
6. Inicie o aplicativo virtual ou a área de trabalho virtual novamente.
7. No log de eventos do sistema da máquina VDA, procure o processo que tentou abrir o canal virtual no seguinte evento:
    - Em um VDA de sessão única, ID de evento 2002 da origem Picadd.
    - Em um VDA de várias sessões, ID de evento 14 da origem Rpm.
8. Faça logoff da sessão.

9. Edite a entrada na configuração da política de lista de permissões de canal virtual para incluir o processo identificado.
10. Reinicie o VDA.
11. Inicie o aplicativo virtual ou desktop virtual para validar que o canal virtual personalizado é aberto com sucesso.

Registro da lista de permissões de canal virtual

Os seguintes eventos são registrados no log de eventos da máquina VDA de sessão única:

Nome do Log	Sistema
ID	2001
Origem	Picadd
Nível	Informação
Descrição	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`

Nome do Log	Sistema
ID	2002
Origem	Picadd
Nível	Aviso
Descrição	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>`

Nome do Log	Sistema
ID	2003
Origem	Picadd
Nível	Informações

Descrição	`<username>` abriu o canal virtual personalizado `<vcName>`

Nome do Log	Sistema
ID	2004
Origem	Picadd
Nível	Aviso
Descrição	`<username>` tentou abrir o canal virtual personalizado `<vcName>`

Os seguintes eventos são registrados no log de eventos da máquina VDA de múltiplas sessões:

Nome do Log	Sistema
ID	13
Origem	Rpm
Nível	Informação
Descrição	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`

Nome do Log	Sistema
ID	14
Origem	Rpm
Nível	Aviso
Descrição	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>`

Nome do Log	Sistema

Id	15
Origem	Rpm
Nível	Informação
Descrição	`<username>` abriu o canal virtual personalizado `<vcName>`

Nome do Log	Sistema
Id	16
Origem	RPM
Nível	Aviso
Descrição	`<username>` tentou abrir o canal virtual personalizado `<vcName>`

Canais virtuais de terceiros conhecidos

A seguir estão soluções de terceiros conhecidas que usam canais virtuais personalizados da Citrix. Esta lista não inclui todas as soluções que usam um canal virtual personalizado da Citrix.

- Cerner
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- Epic Warp Drive
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Reuniões do Zoom para VDI

Para obter detalhes sobre como adicionar os canais virtuais associados à lista de permissões, entre em contato com os fornecedores das soluções. Alternativamente, siga as etapas descritas na seção Obtendo nomes e processos de canais virtuais.

Serviço de Autenticação Federada

O Citrix Federated Authentication Service (FAS) permite o logon único (SSO) para desktops e aplicativos virtuais Citrix em ambientes onde os usuários autenticar por meio de provedores de identidade modernos, como SAML ou OpenID Connect (OIDC), que não fornecem uma senha do Windows, garantindo acesso contínuo a hosts de sessão unidos a um domínio do Active Directory.

Para obter mais informações sobre como proteger sua implantação com o Serviço de Autenticação Federada, consulte a documentação Serviço de Autenticação Federada em seu próprio documento.

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:

- Dispositivo USB genérico
- Dispositivos móveis e de tela sensível ao toque
- Dispositivos seriais
- Teclados especiais
- Dispositivos TWAIN
- Webcams
- Dispositivos WIA

Dispositivo USB otimizado vs. genérico

Um dispositivo USB otimizado é aquele para o qual o aplicativo Citrix Workspace™ tem suporte específico. Por exemplo, a capacidade de redirecionar webcams usando o canal virtual HDX Multimedia. Um dispositivo genérico é um dispositivo USB para o qual não há suporte específico no aplicativo Citrix Workspace.

Por padrão, o redirecionamento USB genérico não pode redirecionar dispositivos USB com suporte a canal virtual otimizado, a menos que sejam colocados no modo Genérico.

Em geral, você obtém melhor desempenho para dispositivos USB no modo Otimizado do que no modo Genérico. No entanto, há casos em que um dispositivo USB não possui funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos seus recursos.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados por políticas Citrix®. As principais diferenças são:

Se 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 habilitados.
- Um dispositivo está configurado para redirecionamento automático.
- Um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão.

Para obter mais informações, consulte `<http://support.citrix.com/article/CTX123015>`.

RECURSO	MAPEAMENTO DE UNIDADE CLIENTE	REDIRECIONAMENTO USB GENÉRICO
Habilitado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado na sessão virtual.	Somente Citrix Virtual Desktops™

DPIs mistos com vários monitores

Os ambientes Citrix Virtual Apps and Desktops não suportam o uso de DPIs diferentes entre monitores. Você pode verificar o DPI (% de escala) usando Painel de Controle do Windows > Opções de Exibição. Se estiver usando um dispositivo cliente Windows 8.1 ou Windows 10, habilitar a opção **Deixar-me escolher um nível de escala para todos os meus monitores** em Painel de Controle do Windows > Opções de Exibição configura os monitores de forma apropriada. Para obter mais informações, consulte o artigo do Knowledge Center CTX201696.

Unidades de cliente mapeadas

Como precaução de segurança, quando um usuário faz logon no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades do cliente sem permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis que residem em unidades de cliente mapeadas, substitua esse padrão editando o registro no servidor. Para obter informações sobre a

configuração do registro, consulte Unidades de cliente mapeadas na lista de recursos gerenciados por meio 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.

Dispositivos USB genéricos

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. Esses dispositivos incluem:

- Monitores
- Mouses
- Teclados
- Telefones de Voz sobre Protocolo de Internet
- Fones de ouvido
- Webcams
- Scanners
- Câmeras
- Impressoras
- Unidades
- Leitores de cartão inteligente
- Mesas digitalizadoras
- Pads de assinatura

O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes de alta latência ou sensíveis à segurança.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde ele é inadequado. Para obter mais informações sobre o redirecionamento USB genérico, consulte Redirecionamento USB genérico.

Para obter mais informações sobre dispositivos USB e o Citrix Workspace app para Windows, consulte Configurando o redirecionamento de dispositivo USB composto e Configurando o suporte a USB.

Suporte para dispositivos cliente móveis e com tela sensível ao toque

Citrix Virtual Apps and Desktops™ permite que os usuários acessem seus aplicativos e desktops publicados a partir de dispositivos cliente móveis e com tela sensível ao toque.

Requisitos

Plano de controle Citrix®

- Citrix Virtual Apps and Desktops 7.15 ou posterior
- Citrix DaaS™

Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: versão 7.15 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Aplicativo Citrix Workspace™ para Windows versão 1808 ou superior

Modo tablet para dispositivos com tela sensível ao toque usando o Windows Continuum

Continuum é um recurso do Windows 10 que se adapta à forma como o dispositivo cliente é usado. Quando o VDA detecta a presença de um teclado ou mouse em um cliente habilitado para toque, ele coloca o cliente no modo desktop. Se um teclado ou mouse não estiver presente, o VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão da sessão e também durante a sessão quando o teclado ou mouse é conectado ou desconectado.

O recurso é habilitado por padrão. Para desabilitar este recurso, configure as configurações de política Configurações de política de alternância do modo tablet.

Além dos requisitos para dispositivos com tela sensível ao toque mencionados acima, os seguintes são necessários para o Windows Continuum:

Citrix Hypervisor™

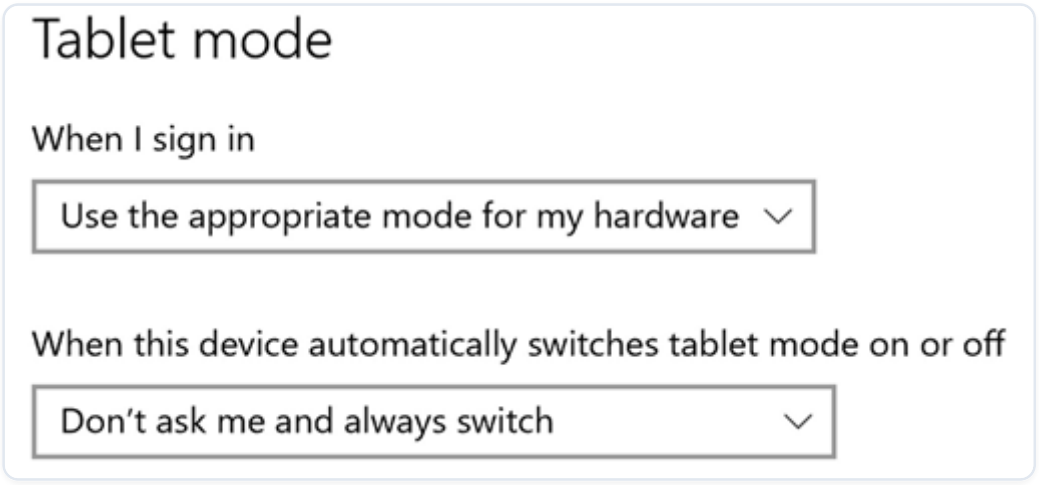
- Citrix Hypervisor 8.2 ou superior
- Execute o comando CLI do XenServer para permitir a alternância entre laptop/tablet: **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **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
- VDA
  - Windows: versão 7.16 ou posterior
  - **Devido às limitações atuais nas configurações do sistema operacional, o usuário terá que definir as seguintes opções nos menus suspensos depois de iniciar a primeira sessão ICA® e reiniciar o VDA:**
    - **Configurações > Sistema > Modo Tablet**
      - Usar o modo apropriado para meu hardware
      - Não me perguntar e sempre alternar



O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores.
- A tela Iniciar e quaisquer aplicativos que você iniciar abrem em tela cheia.
- A barra de tarefas contém um botão Voltar.
- Ícones excluídos da barra de tarefas.

Você tem acesso ao Explorador de Arquivos.



O Windows 10 carrega o driver GPIO na máquina virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro da máquina virtual.

O aplicativo Citrix Workspace para HTML5 não oferece suporte aos recursos do Windows Continuum.

O **modo desktop** oferece a interface de usuário tradicional onde você interage da mesma forma que usaria um PC com teclado e mouse.

Canetas Microsoft Surface Pro e Surface Book

Oferecemos suporte à funcionalidade padrão da caneta com aplicativos baseados em Windows Ink. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e do modelo da caneta. Por exemplo, a pressão da caneta pode ter até 4096 níveis. Este recurso é ativado por padrão.

A seguir estão os requisitos para o suporte à funcionalidade da caneta:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 1903 ou posterior
- Citrix DaaS

Host de sessão

- Sistema Operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2016 ou posterior
  - Windows 11
- VDA
  - Windows: versão 1903 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Aplicativo Citrix Workspace para Windows versão mínima 1902

Para uma demonstração do Windows Ink e da funcionalidade da caneta, clique nesta imagem:



Para desabilitar ou habilitar esse recurso, consulte Canetas Microsoft Surface Pro e Surface Book na lista de recursos gerenciados pelo registro.

Problemas conhecidos

A seguir estão os problemas conhecidos com o suporte à caneta:

- Devido a limitações do 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:**

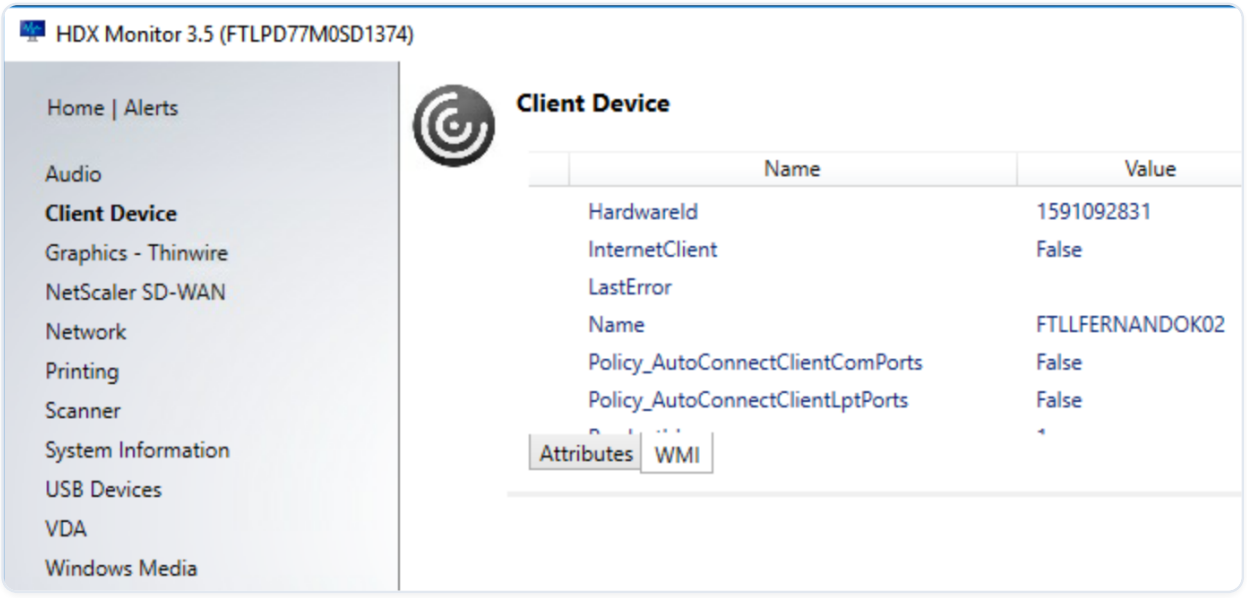
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um pad de assinatura) de forma consistente apenas se ele estiver conectado a COM1 ou COM2 na estação de trabalho cliente.

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 de 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 (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.

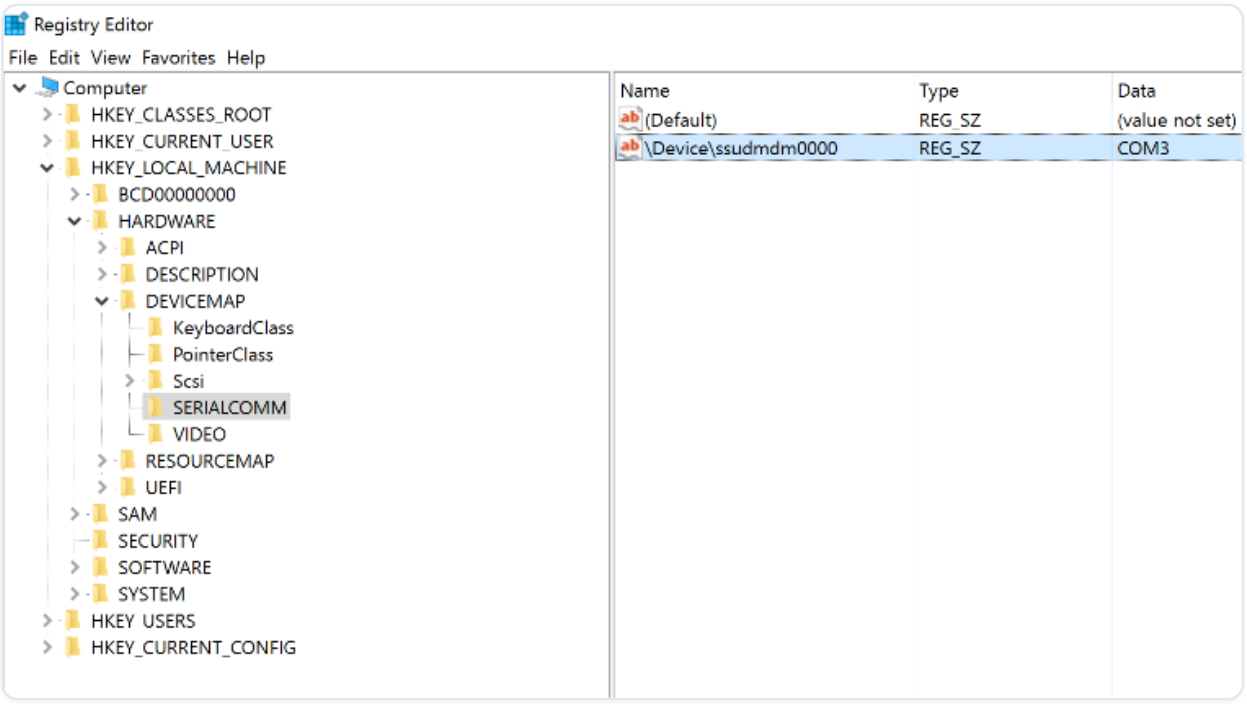
Importante:

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.

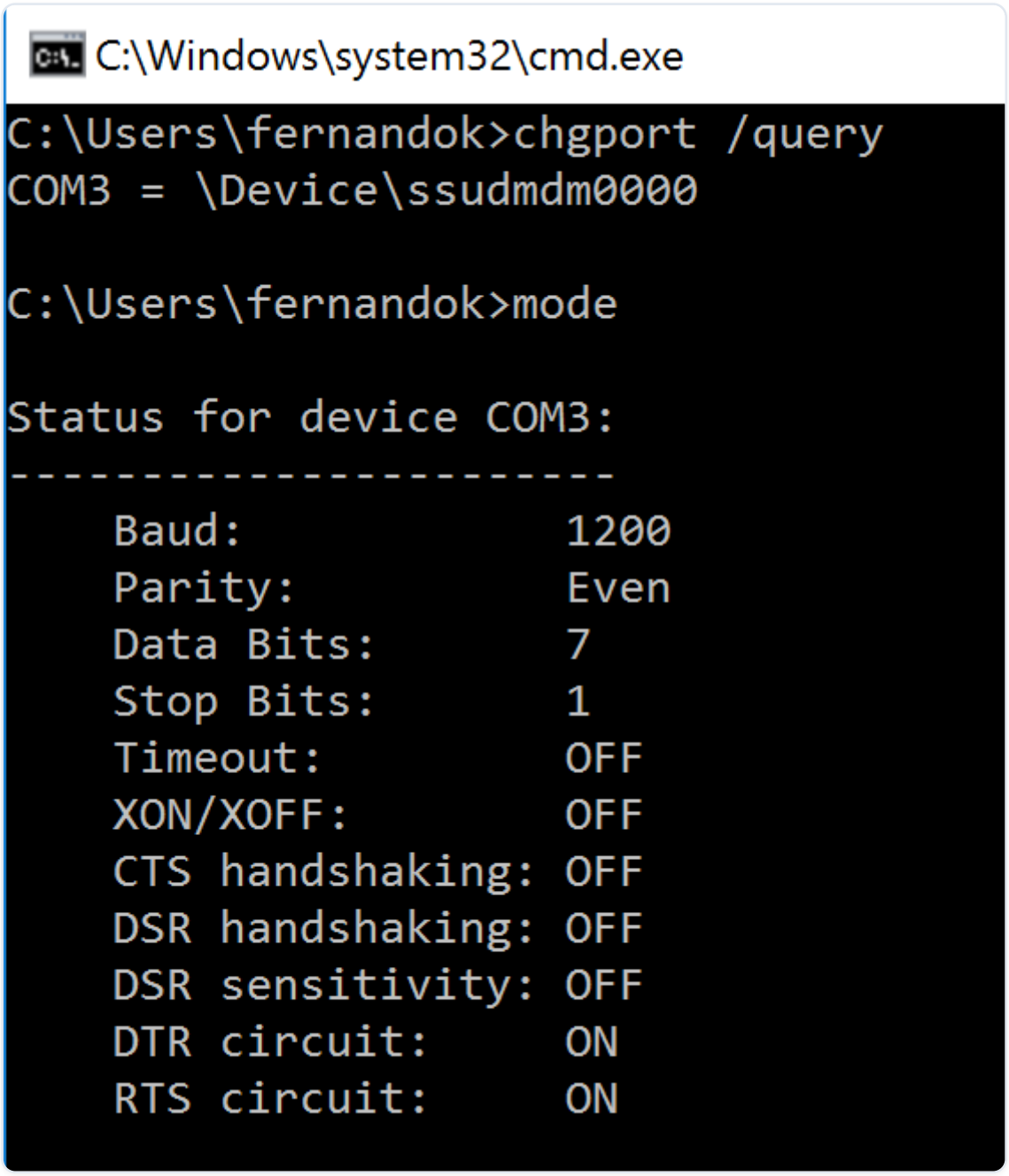
Solução de problemas

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

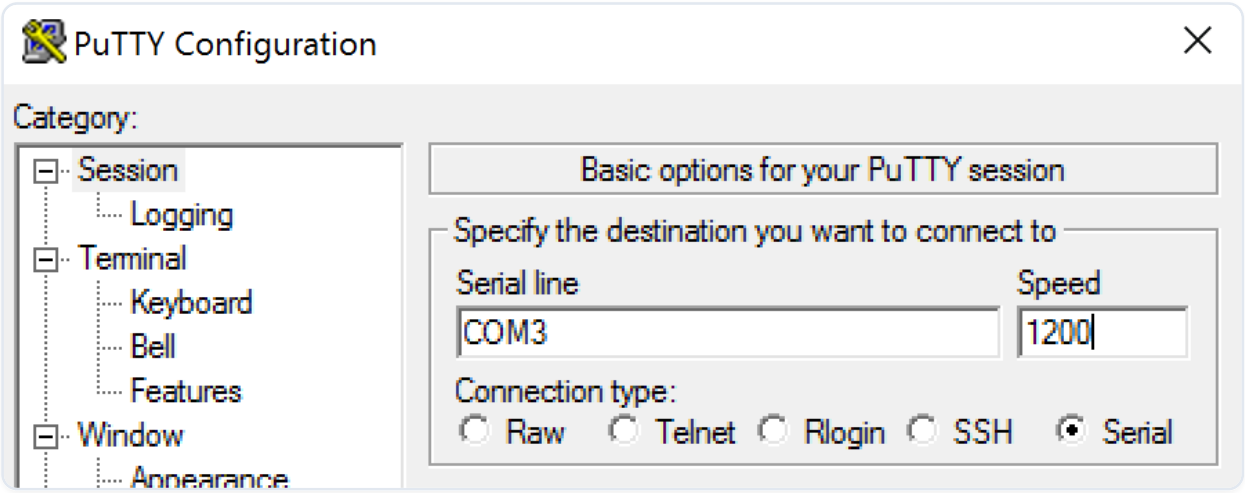
porta COM serial, uma chave de registro é criada no hive mostrado aqui:



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 aos teclados Bloomberg modelo 5, modelo 4 Starboard (e ao modelo 3 anterior). Este teclado permite que os 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 entrada para microfone e fone de ouvido.
- Hub USB para conectar todos esses dispositivos ao sistema.

Requisitos:

- A sessão à qual o aplicativo Citrix Workspace™ para Windows está se conectando deve 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:

- Bloomberg LP Bloomberg Biometric Module
- Bloomberg LP Keyboard (Dispositivo composto com duas interfaces)
- Bloomberg LP Keyboard Audio (Dispositivo composto com três interfaces)

Para teclados Bloomberg 3 e 4:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Cenário somente de aplicativo 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 em cada um desses dispositivos indica que eles são redirecionados para a sessão.

Dispositivos TWAIN

Requisitos

- O scanner deve ser compatível com TWAIN.
- Instale os drivers TWAIN 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 driver TWAIN local e não o serviço de Aquisição de Imagens do Windows.
- 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.

Para obter informações sobre as configurações de política, consulte configurações de política de dispositivos TWAIN.

Webcams

Streaming de webcam de alta definição

Webcams podem ser usadas por aplicativos de videoconferência em execução na sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo de videoconferência. Quando a webcam e o aplicativo suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos resoluções de webcam de até 1920x1080.

Este recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para obter uma lista 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.

Dispositivos WIA

Requisitos

- O scanner deve ser compatível com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, via USB).
- Certifique-se de que o scanner esteja usando o serviço local do Windows Image Acquisition e não o driver TWAIN.
- Certifique-se de que nenhuma política seja aplicada à conta de usuário usada para o teste, e que esteja limitando a largura de banda dentro da sessão ICA®. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Lista de permissões de aplicativos do Windows Image Acquisition

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento de scanner do Windows Image Acquisition. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém o Windows Image Acquisition. Por padrão, nenhum aplicativo tem acesso ao Windows Image Acquisition.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração Lista de permissões de aplicativos do Windows Image Acquisition na lista de recursos gerenciados através do registro.

Para obter informações sobre as configurações de política, consulte Configurações de política de dispositivos WIA.

Gráficos

Os gráficos Citrix HDX incluem um extenso conjunto de tecnologias de aceleração e codificação de gráficos que otimizam a entrega de aplicativos gráficos avançados do Citrix Virtual Apps and Desktops. As tecnologias gráficas proporcionam a mesma experiência de usar um desktop físico ao trabalhar remotamente com aplicativos virtuais que são intensivos em gráficos.

Você pode usar software ou hardware para renderização gráfica. A renderização por software requer uma biblioteca de terceiros chamada rasterizador de software. Por exemplo, o Windows inclui o rasterizador WARP para gráficos baseados em DirectX. Às vezes, você pode querer usar um renderizador de software alternativo. A renderização por hardware (aceleração de hardware) requer um processador gráfico (GPU).

O HDX™ Graphics oferece uma configuração de codificação padrão otimizada para os casos de uso mais comuns. Usando as políticas do Citrix, os administradores de TI também podem configurar várias configurações relacionadas a gráficos para atender a diferentes requisitos e fornecer a experiência de usuário desejada.

Thinwire

Thinwire é a tecnologia de exibição remota padrão do Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição. Os gráficos são gerados como resultado da entrada do usuário, por exemplo, 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 com 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.

Informações relacionadas

- HDX 3D Pro
- Aceleração de GPU para SO de sessão única do Windows
- Aceleração de GPU para SO de múltiplas sessões do Windows
- Framehawk
- Thinwire
- Marca d'água de sessão baseada em texto

HDX™ 3D Pro

Os recursos HDX 3D Pro do Citrix Virtual Apps and Desktops™ permitem que você forneça desktops e aplicativos que têm o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão oferece suporte apenas à aceleração de GPU do DirectX.

Para as configurações de política do HDX 3D Pro, consulte Otimizar para carga de trabalho de gráficos 3D.

Todos os aplicativos Citrix Workspace compatíveis podem ser usados com gráficos 3D. Para obter o melhor desempenho com cargas de trabalho 3D complexas, monitores de alta resolução, configurações de vários monitores e aplicativos de alta taxa de quadros, recomendamos as versões mais recentes do Citrix Workspace app para Windows e do Citrix Workspace app para Linux. Para obter mais informações sobre as versões compatíveis do Citrix Workspace app, consulte Marcos do ciclo de vida do Citrix Workspace app.

Exemplos de aplicativos profissionais 3D incluem:

- Aplicativos de design, fabricação e engenharia assistidos por computador (CAD/CAM/CAE)
- Software de Sistema de Informação Geográfica (GIS)
- Sistema de Comunicação e Arquivamento de Imagens (PACS) para imagens médicas
- Aplicativos que usam as versões mais recentes de OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL

- Aplicativos não gráficos computacionalmente intensivos que usam GPUs NVIDIA Compute Unified Device Architecture (CUDA) para computação paralela

O HDX 3D Pro oferece a melhor experiência do usuário em qualquer largura de banda:

- Em conexões WAN: Ofereça uma experiência de usuário interativa em conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de um desktop local em conexões LAN.

  Você pode substituir estações de trabalho complexas e caras por dispositivos de usuário mais simples, movendo o processamento gráfico para o data center para gerenciamento centralizado.

O HDX 3D Pro fornece aceleração de GPU para máquinas de SO de sessão única do Windows e máquinas de SO de várias sessões do Windows. Para obter mais informações, consulte Aceleração de GPU para SO de sessão única do Windows e Aceleração de GPU para SO de várias sessões do Windows.

O HDX 3D Pro é compatível com as tecnologias de passthrough de GPU e virtualização de GPU oferecidas pelos seguintes hypervisors, além de bare metal:

- Citrix Hypervisor™
  - Passagem de GPU com NVIDIA GRID, AMD e Intel GVT-d
  - Virtualização de GPU com NVIDIA GRID, AMD e Intel GVT-g
  - Consulte a compatibilidade de hardware em Lista de Compatibilidade de Hardware do Hypervisor.

Use a ferramenta HDX Monitor para validar a operação e a configuração das tecnologias de visualização HDX e para diagnosticar e solucionar problemas de HDX. Para baixar a ferramenta e saber mais sobre ela, consulte `<https://taas.citrix.com/hdx/download/>`.

Aceleração de GPU para SO multi-sessão do Windows

HDX™ 3D Pro permite que aplicativos com uso intenso de gráficos executados em sessões do SO multi-sessão 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.

Como o Windows Server é um sistema operacional multiusuário, vários usuários podem compartilhar uma GPU acessada pelo Citrix Virtual Apps™ sem a necessidade de virtualização de GPU (vGPU).

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

Compartilhamento de GPU

O Compartilhamento de GPU permite a renderização de hardware de GPU de aplicativos OpenGL e DirectX em sessões de área de trabalho remota. Ele tem as seguintes características:

- Pode ser usado em máquinas bare metal ou virtuais para aumentar a escalabilidade e o desempenho do aplicativo.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não exige o desempenho de renderização de uma GPU dedicada).
- Não requer configurações especiais.

Uma GPU pode ser atribuída à máquina virtual do Windows Server nos modos de passagem completa (full pass-through) ou GPU virtual (vGPU), seguindo os requisitos do Hypervisor e do fornecedor da GPU. Implantações bare-metal em máquinas físicas do Windows Server também são suportadas.

O Compartilhamento de GPU não depende de nenhuma placa gráfica específica.

- Para máquinas virtuais, selecione uma placa gráfica compatível com o Hypervisor em uso. Para obter uma lista de compatibilidade de hardware do Citrix Hypervisor, consulte Lista de Compatibilidade de Hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de vídeo habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desabilite todas, exceto uma, usando o Gerenciador de Dispositivos.

A escalabilidade usando o Compartilhamento de GPU depende de vários fatores:

- Os aplicativos em execução

- A quantidade de RAM de vídeo que eles consomem
- O poder de processamento da placa gráfica

Alguns aplicativos manipular a escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha do driver da placa gráfica. Limite o número de usuários simultâneos para evitar tais problemas.

Para confirmar que a aceleração da GPU está ocorrendo, use uma ferramenta de terceiros como o GPU-Z. O GPU-Z está disponível em `<http://www.techpowerup.com/gpuz/>`.

- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso e permite o uso de codificação de hardware para codificação H.264 (onde disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política de gráficos.

Renderização DirectX, Direct3D e WPF

A renderização DirectX, Direct3D e WPF está disponível apenas em servidores com uma GPU que suporte uma interface de driver de vídeo (DDI) versão 9ex, 10 ou 11.

- No Windows Server 2008 R2, DirectX e Direct3D não exigem configurações especiais para usar uma única GPU.
- No Windows Server 2012 e posterior, as sessões dos Serviços de Área de Trabalho Remota (RDS) no servidor Host da Sessão RD usam o Microsoft Basic Render Driver como adaptador padrão. Para usar a GPU em sessões RDS no Windows Server 2012 e posterior, habilite a configuração **Usar o adaptador gráfico padrão de hardware para todas as sessões dos Serviços de Área de Trabalho Remota** na política de grupo **Política de Computador Local** \> **Configuração do Computador** \> **Modelos Administrativos** \> **Componentes do Windows** \> **Serviços de Área de Trabalho Remota** \> **Host da Sessão da Área de Trabalho Remota** \> **Ambiente de Sessão Remota**.
- Para permitir que aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no registro do servidor que executa sessões do Windows Multi-session OS. Para obter informações sobre a configuração do registro, consulte Renderização do Windows Presentation Foundation (WPF) na lista de recursos gerenciados através do registro.

Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos POC de aceleração CUDA, habilite as configurações de 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 ou aplicativos hospedados 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 Citrix Hypervisor™, vSphere, Nutanix e Hyper-V (somente passthrough).

O HDX™ 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para desempenho ideal de WAN e sem fio. O HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que suportam NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que suportam NVENC.
- Opção de compressão sem perdas para casos de uso especializados. O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixels são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

  Ao usar 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**.

- 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 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

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

- Suporte a vários monitores e monitores de alta resolução. Para máquinas de SO de sessão única, o HDX 3D Pro oferece suporte a dispositivos de usuário com até quatro monitores. Os

usuários podem organizar seus monitores em qualquer configuração e podem misturar monitores com diferentes resoluções e orientações. O número de monitores é limitado pelos recursos da GPU do computador host, do dispositivo do usuário e da largura de banda disponível. O HDX 3D Pro oferece suporte a todas as resoluções de monitor e é limitado apenas pelos recursos da GPU no computador host.

- Resolução dinâmica. Você pode redimensionar a área de trabalho virtual ou a janela do aplicativo para qualquer resolução. **Nota**: O único método suportado para alterar a resolução é redimensionando a janela da sessão VDA. A alteração da resolução de dentro da sessão VDA (usando **Painel de Controle > Aparência** e **Personalização > Vídeo > Resolução da Tela) não é suportada**.
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro oferece suporte a placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passthrough de GPU e compartilhamento de GPU. O NVIDIA vGPU permite que várias VMs tenham acesso simultâneo e direto a uma única GPU física, usando os mesmos drivers gráficos NVIDIA que são implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar o HDX 3D Pro com vDGA para cargas de trabalho RDS e VDI.
- Suporte para VMware vSphere/ESX usando NVIDIA vGPU e AMD MxGPU.
- Suporte para Microsoft HyperV usando Atribuição de Dispositivo Discreto no Windows Server 2016.
- Suporte para gráficos de data center com a família de processadores Intel Xeon E3. O HDX 3D Pro oferece suporte a vários monitores (até 3), blanking de console, resolução personalizada e alta taxa de quadros com a família de processadores Intel compatível. Para obter mais informações, consulte `<http://www.citrix.com/intel>` e `<http://www.intel.com/content/www/us/en/servers/data-center-graphics.html>`.
- Suporte para AMD RapidFire em placas de servidor AMD FirePro série S. O HDX 3D Pro oferece suporte a vários monitores (até 6), blanking de console, resolução personalizada e alta taxa de quadros. Observação: o suporte do HDX 3D Pro para AMD MxGPU (virtualização de GPU) funciona apenas com vGPUs do VMware vSphere. O Citrix Hypervisor e o Hyper-V são compatíveis com o passthrough de GPU. Para obter mais informações, consulte Solução de Virtualização AMD.
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para codificação H.264 (quando disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação

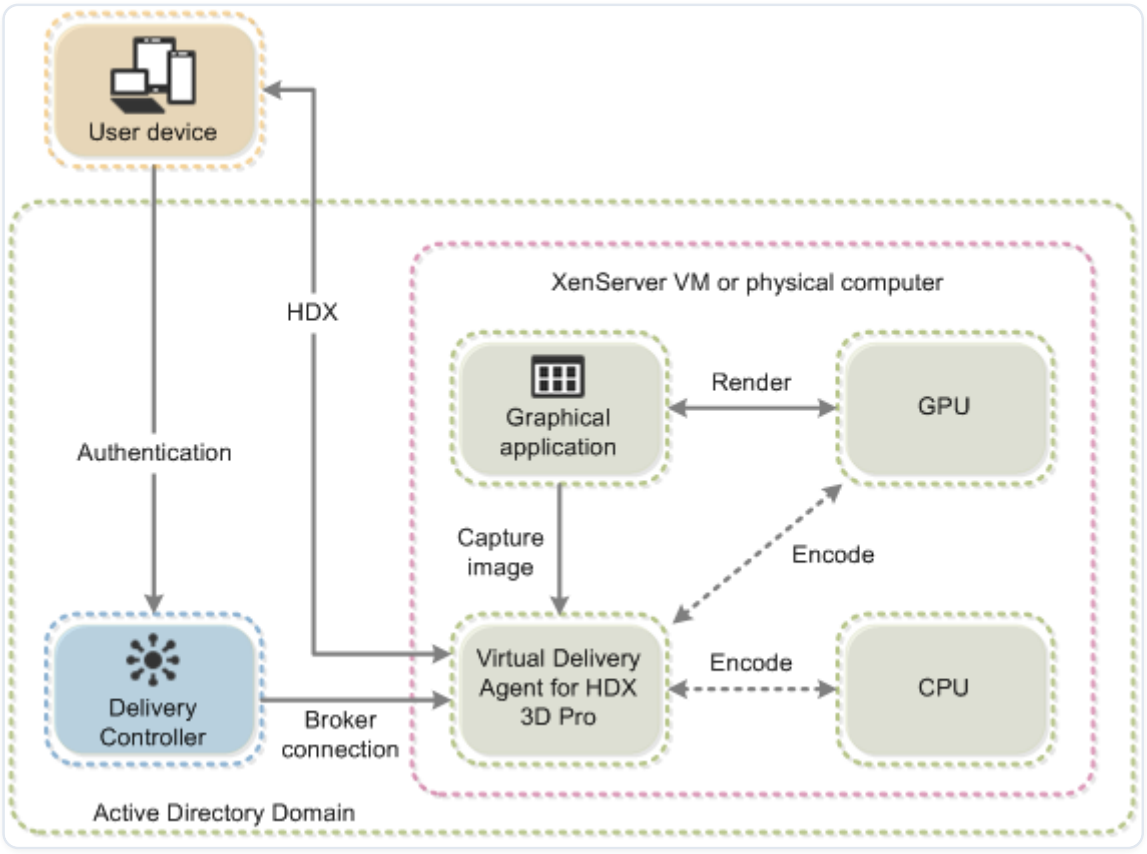
baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política de gráficos.

Conforme mostrado na figura a seguir:

- Quando um usuário faz logon no aplicativo Citrix Workspace™ e acessa o aplicativo ou desktop virtual, o Controller autentica o usuário. O Controller então entra em contato com o VDA para HDX 3D Pro para intermediar uma conexão com o computador que hospeda o aplicativo gráfico.

O VDA para HDX 3D Pro usa o hardware apropriado no host para compactar as visualizações do desktop completo ou apenas do aplicativo gráfico.

- As visualizações do desktop ou aplicativo e as interações do usuário com eles são transmitidas entre o computador host e o dispositivo do usuário. Essa transmissão é feita por meio de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



Otimizar a experiência do usuário do HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política **Limite geral de largura de banda da sessão** para limitar a largura de banda disponível para cada usuário. O uso

dessa configuração garante que a largura de banda disponível não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações na largura de banda disponível ao longo das sessões do usuário podem impactar negativamente o desempenho.

Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a largura de banda necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre.

Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo da Central de Conhecimento CTX128190.

Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais suportado. Em vez disso, use Thinwire com transporte adaptável ativado.

> Framehawk é uma tecnologia especializada de exibição remota para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE) sujeitas a alta perda de pacotes. O Framehawk supera os desafios de interferência espectral e propagação por múltiplos caminhos. O Framehawk oferece uma experiência de usuário fluida e interativa para usuários de aplicativos e desktops virtuais em dispositivos móveis Windows e iOS, como laptops e tablets. Para maximizar a escalabilidade do servidor e minimizar o consumo de largura de banda da rede, recomendamos usar o Framehawk apenas para o caso de uso específico descrito acima. Recomendamos o transporte adaptável, que incorpora muitos conceitos do Framehawk para maximizar o throughput de dados, para todos os outros casos de uso.

Você pode usar modelos de política Citrix® para implementar o Framehawk para um conjunto de usuários e cenários de acesso de uma forma apropriada para sua organização. O Framehawk visa casos de uso móvel de tela única, como laptops e tablets. Use o Framehawk onde o valor

comercial do desempenho interativo em tempo real justifica o custo extra em recursos do servidor e a necessidade de uma conexão de banda larga.

Como o Framehawk mantém uma experiência de usuário suave

Pense no Framehawk como uma implementação de software do olho humano, olhando o que está no buffer de quadros e discernindo os diferentes tipos de conteúdo na tela. O que é importante para o usuário? Quando áreas da tela estão mudando rapidamente, como vídeo ou gráficos em movimento, não importa para o olho humano se alguns pixels são perdidos. Essas áreas são rapidamente sobrescritas com novos dados.

Mas quando se trata de áreas estáticas da tela, o olho humano é exigente. Por exemplo, os ícones na área de notificação ou em uma barra de ferramentas, ou texto depois de rolar para onde o usuário deseja começar a ler. Um usuário espera que essas áreas sejam perfeitas em pixels. Ao contrário dos protocolos que visam ser tecnicamente precisos de uma perspectiva de **uns e zeros**, o Framehawk visa ser relevante para o ser humano que está usando a tecnologia.

O Framehawk inclui um amplificador de sinal de Qualidade de Serviço de próxima geração, além de um mapa de calor baseado em tempo para uma identificação mais granular e eficiente das cargas de trabalho. Ele usa transformações autônomas e de autocorreção, além de compressão de dados, e evita a retransmissão de dados para manter a resposta ao clique, a linearidade e uma cadência consistente. Em uma conexão de rede com perdas, o Framehawk pode ocultar a perda com interpolação, e o usuário ainda percebe boa qualidade de imagem enquanto desfruta de uma experiência mais fluida. Além disso, os algoritmos do Framehawk distinguem inteligentemente entre diferentes tipos de perda de pacotes. Por exemplo, perda aleatória (envie mais dados para compensar) versus perda por congestionamento (não envie mais dados porque o canal já está entupido).

O Framehawk Intent Engine no aplicativo Citrix Workspace™ distingue entre rolar para cima ou para baixo, aplicar zoom, mover para a esquerda ou para a direita, ler, digitar e outras ações comuns. O mecanismo também gerencia a comunicação de volta para o Virtual Delivery Agent (VDA) usando um dicionário compartilhado. Se o usuário estiver tentando ler, a qualidade visual do texto deve ser excelente. Se o usuário estiver rolando, deve ser rápido e suave. E tem que ser interrompível, para que o usuário esteja sempre no controle da interação com o aplicativo ou desktop.

Ao medir a cadência na conexão de rede (**engrenagem**, análoga à tensão em uma corrente de bicicleta), a lógica do Framehawk reage mais rapidamente, proporcionando uma experiência superior em conexões de alta latência. Este sistema de engrenagem exclusivo e patenteado

fornece feedback constante e atualizado sobre as condições da rede, permitindo que o Framehawk reaja imediatamente a mudanças na largura de banda, latência e perda.

Considerações de design usando Thinwire e Framehawk

O Framehawk usa uma camada de transporte de dados construída sobre o (User Datagram Protocol (UDP). O UDP é uma pequena parte de como o Framehawk supera a perda de dados, como você pode ver ao comparar o desempenho do Framehawk com outros protocolos baseados em UDP. O UDP fornece uma base importante para as técnicas centradas no ser humano que diferenciam o Framehawk.

De quanta largura de banda o Framehawk precisa?

O significado de banda larga sem fio depende de vários fatores, incluindo quantos usuários estão compartilhando a conexão, a qualidade da conexão e os aplicativos em uso. Para um desempenho ideal, a Citrix sugere uma base de 4 Mbps ou 5 Mbps mais cerca de 150 Kbps por usuário simultâneo.

Nossa recomendação de largura de banda para Thinwire é geralmente uma base de 1,5 Mbps mais 150 Kbps por usuário. Para detalhes, consulte o blog de largura de banda do Citrix Virtual Apps and Desktops). Com 3% de perda de pacotes, você descobrirá que o Thinwire sobre TCP precisa de muito mais largura de banda do que o Framehawk para manter uma experiência de usuário positiva.

O Thinwire permanece o canal principal de exibição remota no protocolo ICA®. O Framehawk é desativado por padrão. A Citrix recomenda ativá-lo seletivamente para atender aos cenários de acesso sem fio de banda larga em sua organização. Lembre-se de que o Framehawk requer consideravelmente mais recursos do servidor (CPU e memória) do que o Thinwire.

Requisitos e considerações

O Framehawk requer VDA 7.6.300 e Gerenciamento de Política de Grupo 7.6.300 no mínimo.

O endpoint deve ter no mínimo Workspace app para Windows 1808, ou Citrix Receiver para Windows 4.3.100, Workspace app para iOS 1808, ou Citrix Receiver para iOS 6.0.1.

Por padrão, o Framehawk usa um intervalo de portas bidirecional do User Datagram Protocol (UDP) (3224 a 3324) para trocar dados do canal de exibição do Framehawk com o aplicativo Citrix Workspace. O intervalo pode ser personalizado em uma configuração de política chamada **Framehawk display channel port range**. Cada conexão simultânea entre o cliente e o desktop virtual requer uma porta exclusiva. Para ambientes de SO multiusuário, como servidores Citrix

Virtual Apps™, defina portas suficientes para suportar o número máximo de sessões de usuário simultâneas. Para um SO de usuário único, como desktops VDI, é suficiente definir uma única porta UDP. O Framehawk tenta usar a primeira porta definida, trabalhando até a porta final especificada no intervalo. Isso se aplica tanto ao passar pelo Citrix Gateway quanto às conexões internas diretamente para o servidor StoreFront.

Para acesso remoto, um Citrix Gateway deve ser implantado. Por padrão, o Citrix Gateway usa a porta UDP 443 para comunicação criptografada entre o aplicativo Citrix Workspace do cliente e o Gateway. Esta porta deve estar aberta em quaisquer firewalls externos para permitir comunicação segura em ambas as direções. O recurso é conhecido como Datagram Transport Security (DTLS).

> **Observação:**

> As conexões Framehawk/DTLS não são suportadas em dispositivos FIPS.

> As conexões Framehawk criptografadas são suportadas, a partir do NetScaler Gateway versão 11.0.62 e do NetScaler Unified Gateway versão 11.0.64.34 ou posterior.

A Alta Disponibilidade do NetScaler é suportada a partir do XenApp e XenDesktop 7.12.

Considere as seguintes recomendações antes de implementar o Framehawk:

- Entre em contato com o administrador de segurança para confirmar se as portas UDP definidas para o Framehawk estão abertas no firewall. O processo de instalação não configura automaticamente o firewall.
- Frequentemente, o Citrix Gateway pode ser instalado na DMZ, ladeado por firewalls nos lados externo e interno. Certifique-se de que a porta UDP 443 esteja aberta no firewall externo. Certifique-se de que as portas UDP 3224 a 3324 estejam abertas no firewall interno se o ambiente estiver usando os intervalos de portas padrão.

Configuração

> **Cuidado:**

> A Citrix recomenda que você habilite o Framehawk apenas para usuários que provavelmente experimentarão alta perda de pacotes. Também recomendamos que você não habilite o Framehawk como uma política universal para todos os objetos no Site.

> O Framehawk é desativado por padrão. Quando ativado, o servidor tenta usar o Framehawk para gráficos e entrada do usuário. Se os pré-requisitos não forem atendidos por qualquer motivo, a conexão será estabelecida usando o modo padrão (Thinwire).

As seguintes configurações de política afetam o Framehawk:

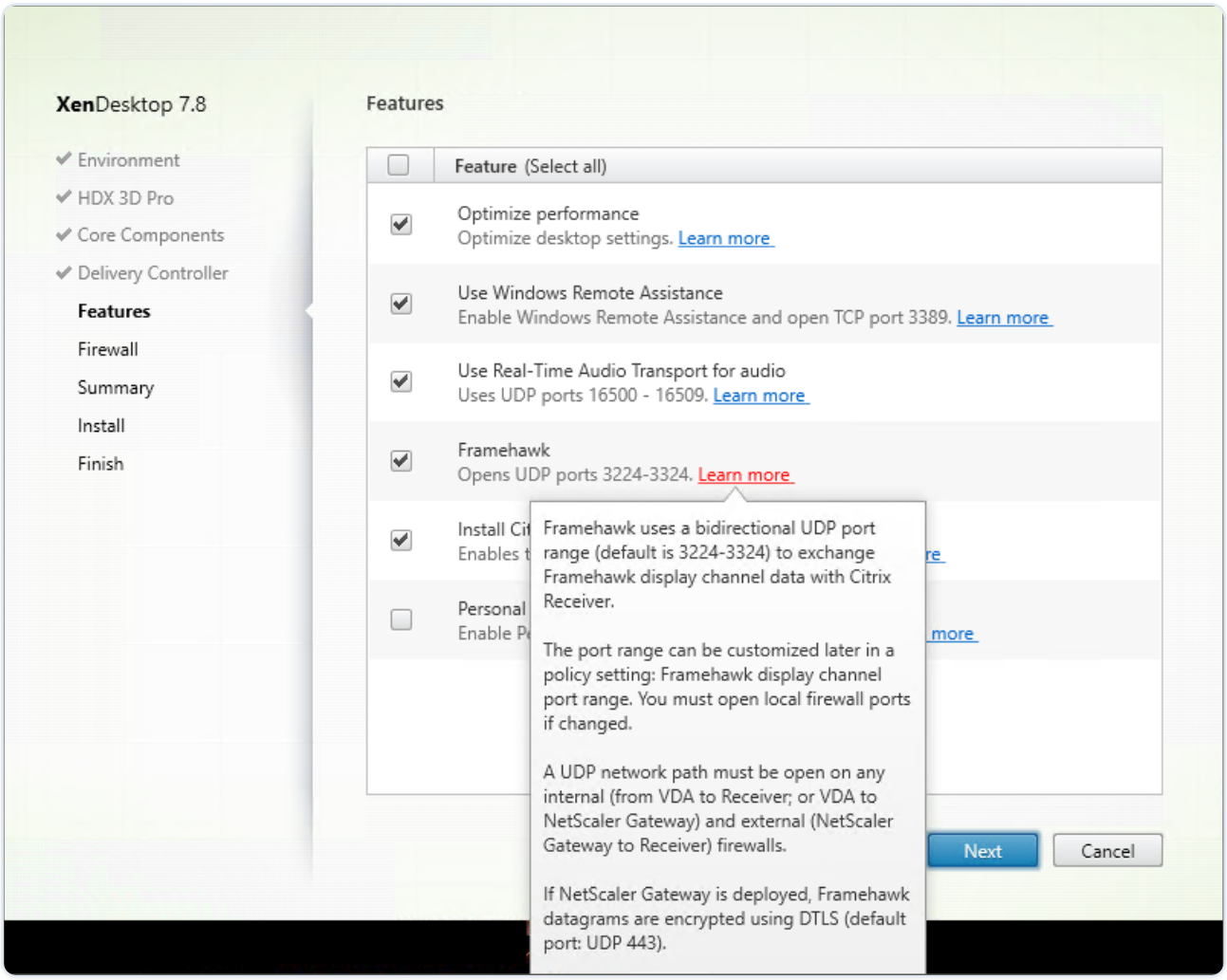
- Canal de exibição Framehawk: Ativa ou desativa o recurso.
- Intervalo de portas do canal de exibição Framehawk: Especifica o intervalo de números de porta UDP (do menor ao maior número de porta) que o VDA usa para trocar dados do canal de exibição Framehawk com o dispositivo do usuário. O VDA tenta usar cada porta, começando pelo menor número de porta e incrementando a cada tentativa subsequente. A porta lida com tráfego de entrada e saída.

Abrindo portas para o canal de exibição Framehawk

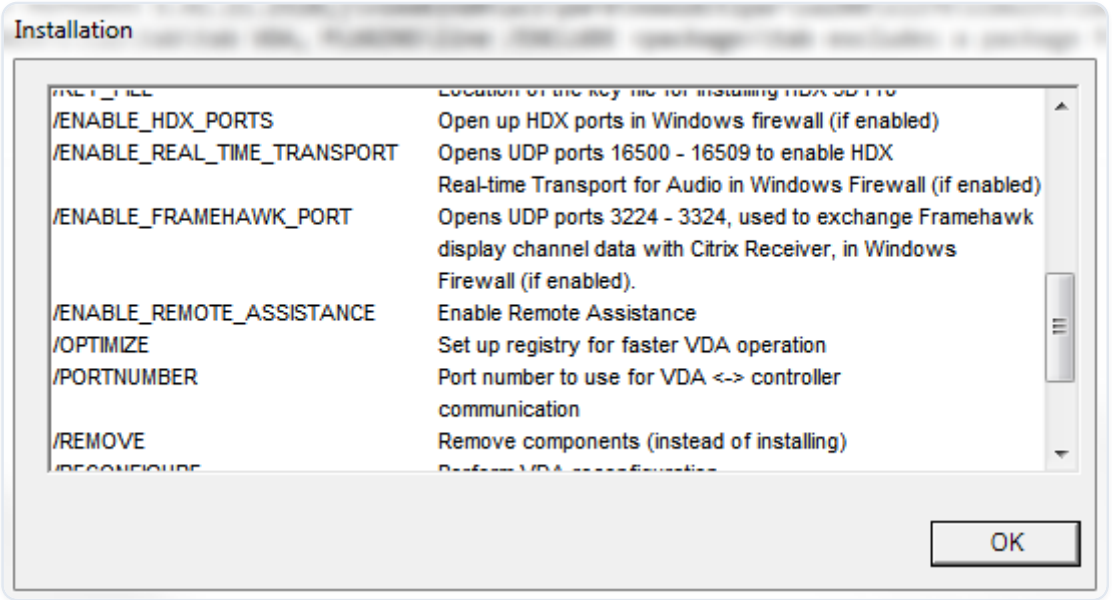
A partir do XenApp e XenDesktop 7.8, uma opção está disponível para reconfigurar o Firewall durante a etapa de **Recursos** do instalador do VDA. Esta caixa de seleção abre as portas UDP 3224 a 3324 no Firewall do Windows, se selecionada. A configuração manual do Firewall é necessária em algumas circunstâncias:

- Para quaisquer Firewalls de rede. Ou
- O intervalo de portas padrão é personalizado.

Para abrir essas portas UDP, selecione a caixa de seleção **Framehawk**:

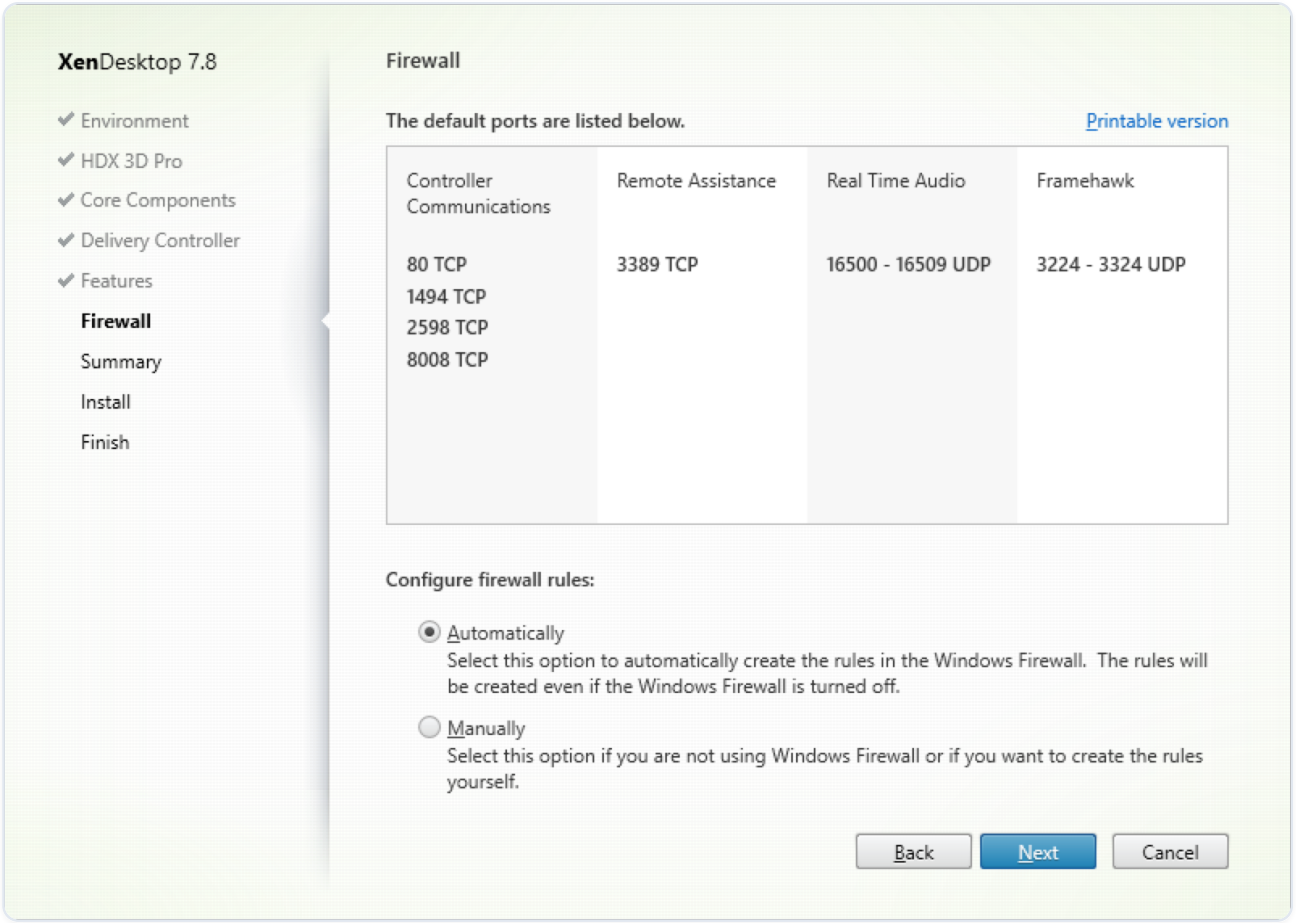


Você também pode usar a linha de comando para abrir portas UDP para Framehawk usando */* **ENABLE_FRAMEHAWK_PORT**:

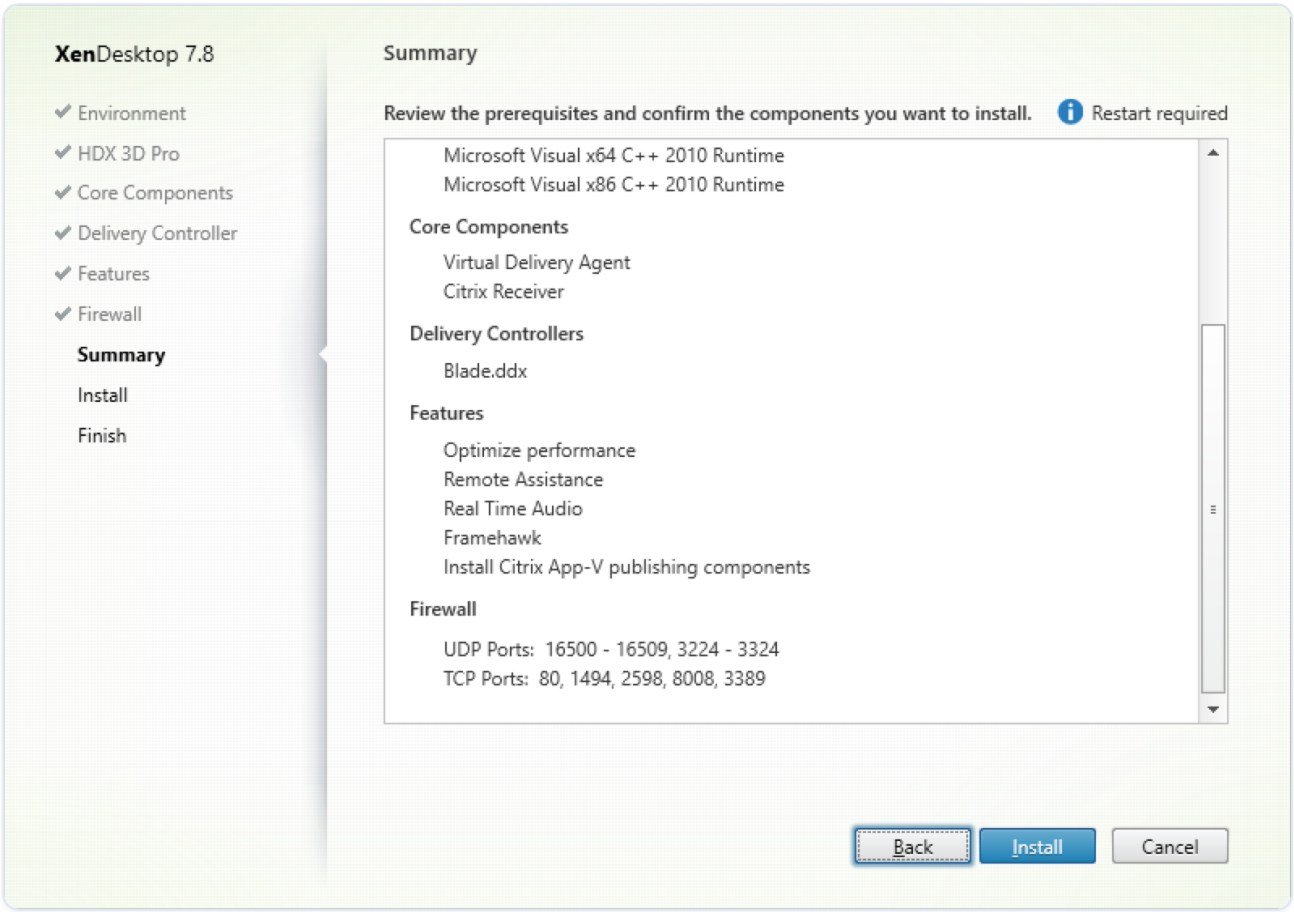


Verificando atribuições de porta UDP do Framehawk

Durante a instalação, você pode verificar as portas UDP atribuídas ao Framehawk na tela **Firewall**:



A tela **Resumo** indica se o recurso Framehawk está ativado:



Suporte do Citrix Gateway para Framehawk

O tráfego Framehawk criptografado é compatível com Citrix Gateway 1808 ou posterior e NetScaler Gateway 11.0.62.10 ou posterior, e Citrix Unified Gateway 1808 e NetScaler Unified Gateway 11.0.64.34 ou posterior.

- Citrix Gateway refere-se à arquitetura de implantação onde o servidor virtual VPN do Gateway é diretamente acessível a partir do dispositivo do usuário final. Ou seja, o servidor virtual VPN tem um endereço IP público atribuído e o usuário se conecta diretamente a este endereço IP.
- Citrix Gateway com Unified Gateway refere-se à implantação onde o servidor virtual VPN do Gateway é vinculado como um destino ao servidor virtual de Comutação de Conteúdo (CS). Nesta implantação, o servidor virtual CS tem o endereço de protocolo de internet público e o servidor virtual VPN do Gateway tem um endereço de protocolo de internet fictício.

Para habilitar o suporte Framehawk no Citrix Gateway, o parâmetro DTLS no nível do servidor virtual VPN do Gateway deve ser habilitado. Depois que o parâmetro é habilitado e os componentes no Citrix Virtual Apps ou Citrix Virtual Desktops™ são atualizados corretamente, o tráfego de áudio, vídeo e interativo do Framehawk é criptografado entre o servidor virtual VPN do Gateway e o dispositivo do usuário.

Citrix Gateway, Unified Gateway e Citrix Gateway + balanceamento de carga de servidor global são compatíveis com Framehawk.

Os seguintes cenários não são compatíveis com Framehawk:

- HDX™ Insight
- Citrix Gateway no modo IPv6
- Citrix Gateway Double Hop
- Citrix Gateway com configuração de Cluster

CENÁRIO	SUPORTE FRAMEHAWK
Citrix Gateway	Sim
Citrix Gateway + balanceamento de carga de servidor global	Sim
Citrix Gateway com Unified Gateway	Sim. **Nota:** A versão 11.0.64.34 ou posterior do Unified Gateway é compatível.
HDX Insight	Não
Citrix Gateway no modo IPv6	Não
Citrix Gateway Double Hop	Não
Múltiplas Autoridades de Ticket Seguro no Citrix Gateway	Sim
Citrix Gateway e Alta Disponibilidade	Sim
Citrix Gateway e configuração de Cluster	Não

Configurando o Citrix Gateway para suporte Framehawk

Para habilitar o suporte ao Framehawk no Citrix Gateway, habilite o parâmetro DTLS no nível do *servidor virtual* VPN do Gateway. Depois que o parâmetro é habilitado e os componentes no Citrix Virtual Apps and Desktops™ são atualizados corretamente, o tráfego de áudio, vídeo e interativo do Framehawk é criptografado entre o servidor virtual VPN do Gateway e o dispositivo do usuário.

Essa configuração é necessária se você estiver habilitando a criptografia UDP no Citrix Gateway para acesso remoto.

Ao configurar o Citrix Gateway para suporte Framehawk:

- Certifique-se de que a porta UDP 443 esteja aberta em quaisquer firewalls externos
- Certifique-se de que a porta CGP (padrão 2598) esteja aberta em quaisquer firewalls externos
- Habilite o DTLS nas configurações do servidor virtual VPN
- Desvincule e revincule o par de certificado-chave SSL. Esta etapa não é necessária se você estiver usando o Citrix Gateway 1808 ou posterior ou o NetScaler versão 11.0.64.34 ou posterior.

Para configurar o Citrix Gateway para suporte Framehawk:

1. Implante e configure o Citrix Gateway para se comunicar com o StoreFront™ e autenticar usuários para Citrix Virtual Apps and Desktops.
2. Na guia Configuração do Citrix Gateway, expanda Citrix Gateway e selecione **Virtual Servers**.
3. Escolha **Edit** para exibir as Configurações Básicas do Servidor Virtual VPN; verifique o estado da configuração DTLS.
4. Escolha **More** para exibir mais opções de configuração:
5. Escolha **DTLS** para fornecer segurança de comunicação para protocolos de datagrama como o Framehawk. Clique em **OK**. A área de Configurações Básicas para o Servidor Virtual VPN mostra que o sinalizador DTLS está definido como **True**.
6. Reabra a tela de Vinculação de Certificado do Servidor e clique em **+** para vincular o par de chaves do certificado.
7. Escolha o par de chaves do certificado anterior, clique em **Select**.
8. Salve as alterações na vinculação do certificado do servidor.
9. Após salvar, o par de chaves do certificado aparece. Clique em **Bind**.
10. Ignore a mensagem de aviso **No usable ciphers configured on the SSL vserver/service**, se ela aparecer.

Etapas para versões mais antigas do NetScaler® Gateway

Se você estiver usando uma versão do NetScaler Gateway anterior a 11.0.64.34:

1. Reabra a tela de Vinculação de Certificado do Servidor e clique em + para vincular o par de chaves do certificado.
2. Escolha o par de chaves do certificado anterior, clique em **Select**.
3. Salve as alterações na vinculação do certificado do servidor.

4. Após salvar, o par de chaves do certificado aparece. Clique em **Vincular**.
5. Ignore a mensagem de aviso **Nenhum cifra utilizável configurada no vserver/serviço SSL**, se ela aparecer.

Para configurar o Unified Gateway para suporte ao Framehawk:

1. Certifique-se de que o Unified Gateway esteja instalado e configurado corretamente. Para obter informações adicionais, consulte as informações sobre Unified Gateway no site de Documentação de Produtos Citrix.
2. Habilite o parâmetro DTLS no *servidor virtual* VPN, que está vinculado ao *servidor virtual* CS como *servidor virtual* de Destino.

Limitações

Se houver entradas DNS obsoletas para o servidor virtual do Citrix Gateway no dispositivo cliente, o transporte adaptativo e o Framehawk podem retornar ao transporte TCP em vez do transporte UDP. Se ocorrer o retorno ao transporte TCP, limpe o cache DNS no cliente e reconecte para estabelecer a sessão usando o transporte UDP.

O Framehawk não oferece suporte a cursores de mouse de 32 bits, como os encontrados em aplicativos como o PTC Creo.

O Framehawk foi projetado para dispositivos móveis, como laptops e tablets usando um único monitor, e ele reverte para o Thinwire em uma configuração de monitor duplo/múltiplo.

Suporte para outros produtos VPN

O Citrix Gateway é o único produto SSL VPN a suportar a criptografia UDP exigida pelo Framehawk. Se outro SSL VPN ou uma versão incorreta do Citrix Gateway for usado, a política do Framehawk pode falhar ao ser aplicada. Produtos VPN IPsec tradicionais suportam Framehawk sem quaisquer modificações.

Monitorando o Framehawk

Você pode monitorar o uso e o desempenho do Framehawk a partir do Citrix Director. A visualização Detalhes do Canal Virtual HDX contém informações úteis para solucionar problemas e monitorar o Framehawk em qualquer sessão. Para visualizar métricas relacionadas ao Framehawk, selecione **Gráficos-Framehawk**.

Se a conexão Framehawk for estabelecida, você verá **Provedor = VD3D** e **Conectado = Verdadeiro** na página de detalhes. É normal que o estado do canal virtual esteja ocioso, pois ele

monitora o canal de sinalização, que é usado apenas durante o handshake inicial. Esta página também fornece outras estatísticas úteis sobre a conexão.

Se você encontrar problemas, consulte o blog de solução de problemas do Framehawk.

Thinwire

Introdução

Thinwire, parte da tecnologia Citrix HDX, é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição.

Uma solução de exibição remota bem-sucedida oferece uma experiência de usuário altamente interativa, semelhante à de um PC local. O Thinwire alcança essa experiência usando uma variedade de técnicas complexas e eficientes de análise e compressão de imagem. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de exibição remota.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso de negócios gerais e é usado como a tecnologia de exibição remota padrão no Citrix Virtual Apps and Desktops.

HDX™ 3D Pro

Em sua configuração padrão, o Thinwire pode fornecer gráficos 3D ou altamente interativos e usar uma unidade de processamento gráfico (GPU), se presente. No entanto, recomendamos habilitar o modo HDX 3D Pro usando as políticas **Otimizar para carga de trabalho de gráficos 3D** ou **Qualidade visual > Construir para sem perdas** para cenários em que GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264 ou H.265) para codificar a tela inteira usando aceleração de hardware se uma GPU estiver presente. Isso proporciona uma experiência mais fluida para gráficos profissionais 3D. Para obter mais informações, consulte H.264 Build to lossless, HDX 3D Pro e Aceleração de GPU para Windows Single-session OS.

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 de configurações de política recomendadas pela Citrix para esses casos de uso.

> **Observação:**
>
> Não oferecemos suporte ao modo gráfico legado nesta versão. Ele está incluído para compatibilidade com versões anteriores ao usar XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões VDA anteriores com Windows 7 e Windows 2008 R2.

- 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 ou 16 bits para uso reduzido de largura de banda. O suporte para tais recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos do servidor (CPU, memória) em cenários de vários monitores e alta resolução. É possível ajustar a quantidade de recursos que o Thinwire usa, no entanto, o uso da largura de banda pode aumentar como resultado.
- Em cenários de baixa largura de banda ou alta latência, considere habilitar gráficos de 8 ou 16 bits para melhorar a interatividade. A qualidade visual pode ser afetada, especialmente em profundidade de cor de 8 bits.

Métodos de codificação

O Thinwire pode operar em dois modos de codificação diferentes, dependendo da política e dos recursos do cliente:

- Thinwire tela cheia H.264 ou H.265
- Thinwire com H.264 ou H.265 seletivo

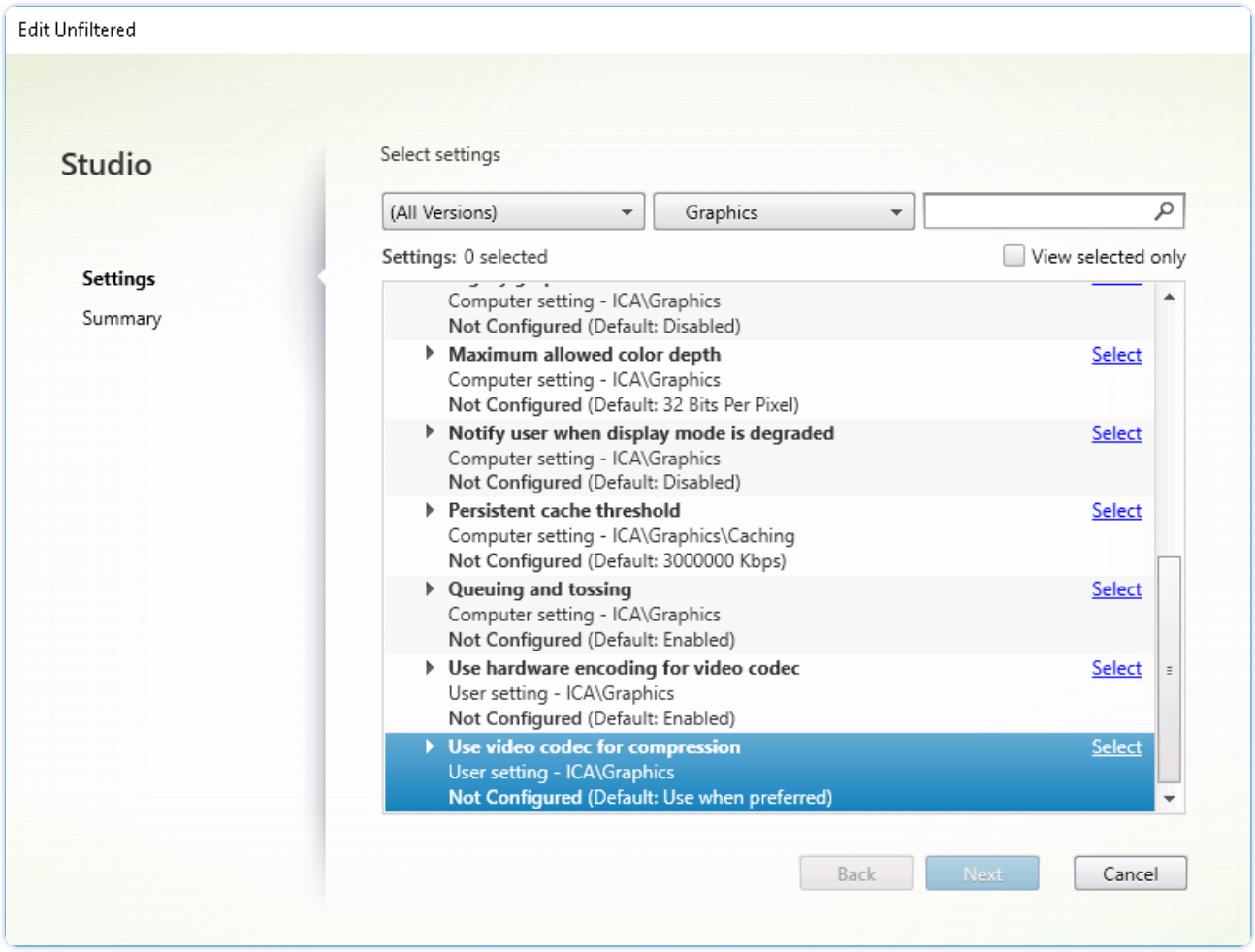
O remoting GDI legado usa o driver de remoting XPDM e não um codificador de bitmap Thinwire.

Configuração

Thinwire é a tecnologia de remoting de exibição padrão.

A seguinte configuração de política de Gráficos define o padrão e fornece alternativas para diferentes casos de uso:

- Usar codec de vídeo para compactação
  - **Usar codec de vídeo quando preferencial**. Esta é a configuração padrão. Nenhuma configuração adicional é necessária. Manter esta configuração como padrão garante que o Thinwire seja selecionado para todas as conexões Citrix e seja otimizado para escalabilidade, largura de banda e qualidade de imagem superior para cargas de trabalho de desktop típicas. Isso é funcionalmente equivalente a **Para regiões em mudança ativa**.
- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:
  - **Para regiões em mudança ativa**. A tecnologia de exibição adaptativa no Thinwire identifica imagens em movimento (vídeo, 3D em movimento) e usa H.264 ou H.265 apenas na parte da tela onde a imagem está se movendo.
  - **Para a tela inteira**. Oferece Thinwire com H.264 ou H.265 em tela cheia para otimizar a experiência do usuário e a largura de banda em casos de uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visualmente sem perdas** está desabilitada), a imagem final não é perfeita em pixels (sem perdas) e pode não ser adequada para certos cenários. Nesses casos, considere usar H.264 Construir para sem perdas em vez disso.



Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de remoting de exibição. O Thinwire as suporta todas.

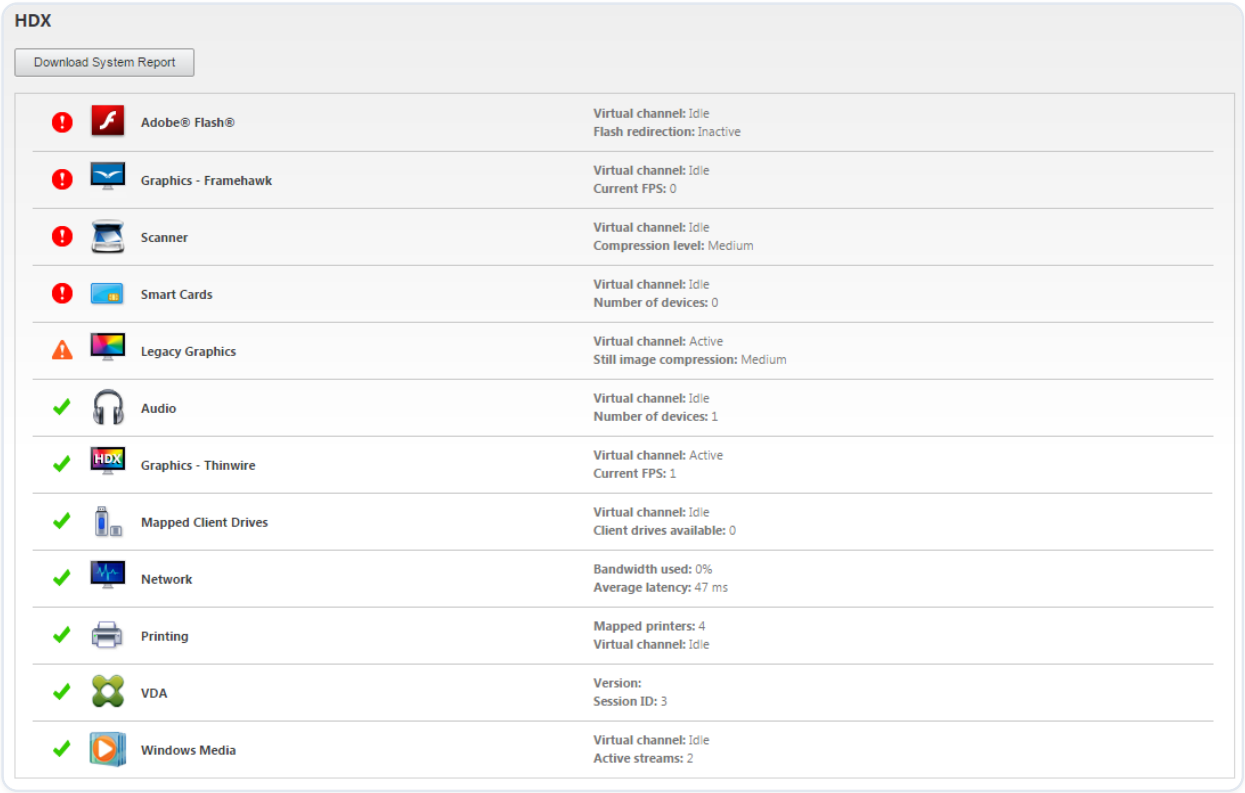
- Profundidade de cor preferida para gráficos simples
- Taxa de quadros alvo
- Qualidade visual

Para obter as combinações recomendadas pela Citrix de configurações de política para diferentes casos de uso de negócios, use os modelos de política da Citrix incorporados. Os modelos **Alta Escalabilidade de Servidor** e **Experiência de Usuário de Altíssima Definição** usam o Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos seus usuários.

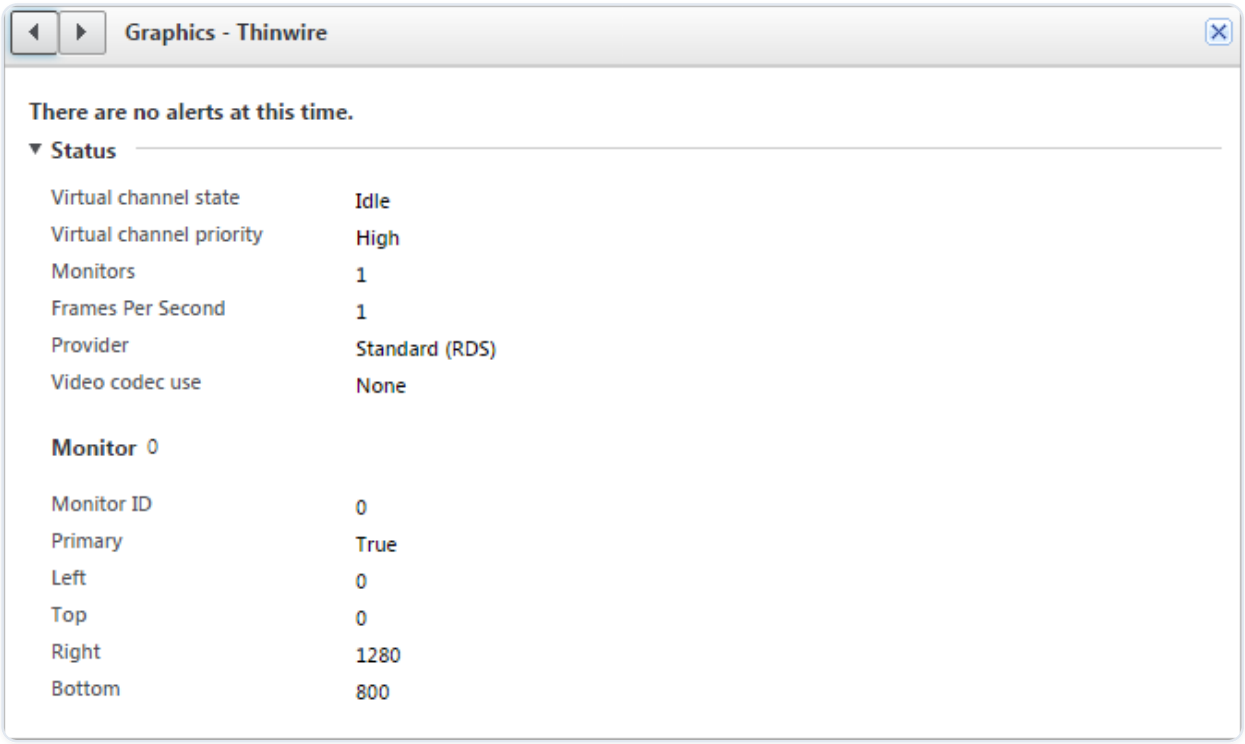
Monitorando o Thinwire

Você pode monitorar o uso e o desempenho do Thinwire 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 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 **Gráficos - Thinwire**.



Codec de compressão sem perdas (MDRLE)

Em uma sessão de desktop típica, a maioria das imagens são gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas usando o codec 2DRLE. No lado do cliente do aplicativo Citrix Workspace, esses elementos são decodificados usando o decodificador 2DRLE do lado do aplicativo Citrix Workspace para exibição da sessão.

No XenApp e XenDesktop 7.17, adicionamos um codec MDRLE com taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este novo codec não afeta a escalabilidade do servidor.

Menor largura de banda geralmente significa interatividade de sessão aprimorada (especialmente em links compartilhados ou restritos) e custos reduzidos. Por exemplo, o consumo de largura de banda esperado ao usar o codec MDRLE é aproximadamente 10–15% menor em comparação com o XenApp e XenDesktop 7.15 LTSR para cargas de trabalho típicas semelhantes ao Office.

A configuração não é necessária para o codec MDRLE. Se o aplicativo Citrix Workspace suportar a decodificação MDRLE, o VDA usará a codificação MDRLE do VDA e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA retornará automaticamente à codificação 2DRLE.

Requisitos do MDRLE:

- Citrix Virtual Apps and Desktops versão mínima 7 1808 VDAs
- XenApp e XenDesktop versão mínima 7.17 VDAs
- Aplicativo Citrix Workspace para Windows versão mínima 1808
- Citrix Receiver para Windows versão mínima 4.11

Modo Progressivo

O Citrix Virtual Apps and Desktops 1808 introduziu o modo progressivo e o ativou por padrão. Em condições de rede restritas (padrão: largura de banda < 2 Mbps ou latência > 200 ms), o Thinwire aumentou a compactação de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens fortemente compactados são então progressivamente aprimorados, de forma aleatória em blocos, quando a atividade da tela é interrompida. Embora compactar e aprimorar dessa forma melhore a interatividade geral, isso reduz a eficiência do cache e aumenta o uso da largura de banda.

A partir do Citrix Virtual Apps and Desktops 1906, o modo progressivo é desativado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada nas

condições da rede e flutua entre um valor mínimo e máximo predefinido para cada configuração de **Qualidade visual**. Como não há uma etapa explícita de aprimoramento, o Thinwire otimiza a entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

Alterando o comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a chave do registro. Para obter informações, consulte Modo progressivo na lista de recursos gerenciados por meio do registro.

H.264 Construção para sem perdas

Construção 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 **Construção para sem perdas**.

A Construção para sem perdas compacta a tela usando H.264 (ou H.265) durante a atividade da tela e aprimora para pixel perfeito (sem perdas) quando a atividade para. A qualidade da imagem H.264 (ou H.265) se adapta aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de aprimoramento é realizada gradualmente, proporcionando uma resposta imediata se o usuário iniciar a atividade da tela logo após o início do aprimoramento. Por exemplo, selecionar um modelo e girá-lo.

O H.264 **Construção para sem perdas** oferece todas as vantagens do H.264 ou H.265 em tela cheia, incluindo aceleração de hardware, mas com o benefício adicional de uma tela final garantida sem perdas. Isso é fundamental para cargas de trabalho do tipo 3D que exigem uma imagem final perfeita em pixels. Por exemplo, manipular imagens médicas. Além disso, o H.264 **Construção para sem perdas** usa menos recursos do que o H.264 4:4:4 em tela cheia. Como resultado, usar a **Construção para sem perdas** geralmente resulta em uma taxa de quadros mais alta do que o H.264 4:4:4 visualmente sem perdas.

> **Observação:**
>
> Além da política de **Qualidade visual**, defina a política **Usar codec de vídeo** como **Usar quando preferencial** (padrão) ou **Para regiões em mudança ativa**. Você pode reverter para a Construção para sem perdas não H.264 definindo a política **Usar codec de vídeo** como **Não usar codec de vídeo**. Isso resulta em imagens em movimento sendo codificadas com JPEG em vez de H.264 (ou H.265).

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e a permitir o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que é uma camada de texto, 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 VDA.

> **Importante:**

> A marca d'água de sessão baseada em texto não é um recurso de segurança. A solução não impede completamente o roubo de dados, mas oferece algum nível de impedimento e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar esse recurso, recomendamos que você o combine com outras soluções de segurança, conforme aplicável.

> A marca d'água da sessão é um texto e é aplicada à sessão que é entregue ao usuário. A marca d'água da sessão contém informações para rastrear o roubo de dados. Os dados mais importantes são a identidade do usuário de logon da sessão atual na qual a imagem da tela foi capturada. Para rastrear o vazamento de dados de forma mais eficaz, inclua outras informações, como o endereço IP do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as configurações de política de Marca d'água da sessão para configurar o posicionamento e a aparência da marca d'água na tela.

Requisitos:

Virtual Delivery Agents:

SO multissessão 7.17 SO de sessão única 7.17

Limitações:

- As marcas d'água de sessão não são suportadas em sessões onde 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 da 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 essas 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 **Ativado 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 a Gravação de Sessão, 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 inclui as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

Compartilhamento de tela

O compartilhamento de tela permite que um usuário compartilhe uma sessão do Citrix Virtual Desktop com outros, incluindo conteúdo da tela, teclado e controles do mouse.

Requisitos do sistema

- Windows: VDA de SO de sessão única ou multi-sessão
- Linux: Consulte a documentação do VDA Linux para obter mais informações sobre o compartilhamento de sessões Linux.
- Apenas sessões de desktop podem ser compartilhadas.
- Deve haver conectividade de rede entre o VDA que hospeda a sessão e as máquinas que se conectam às sessões compartilhadas. Os requisitos de porta de rede são baseados nas portas

ICA em uso (TCP/UDP 1494 ou 2598) e na configuração da política de compartilhamento de tela (TCP 52525 a 52625 por padrão).

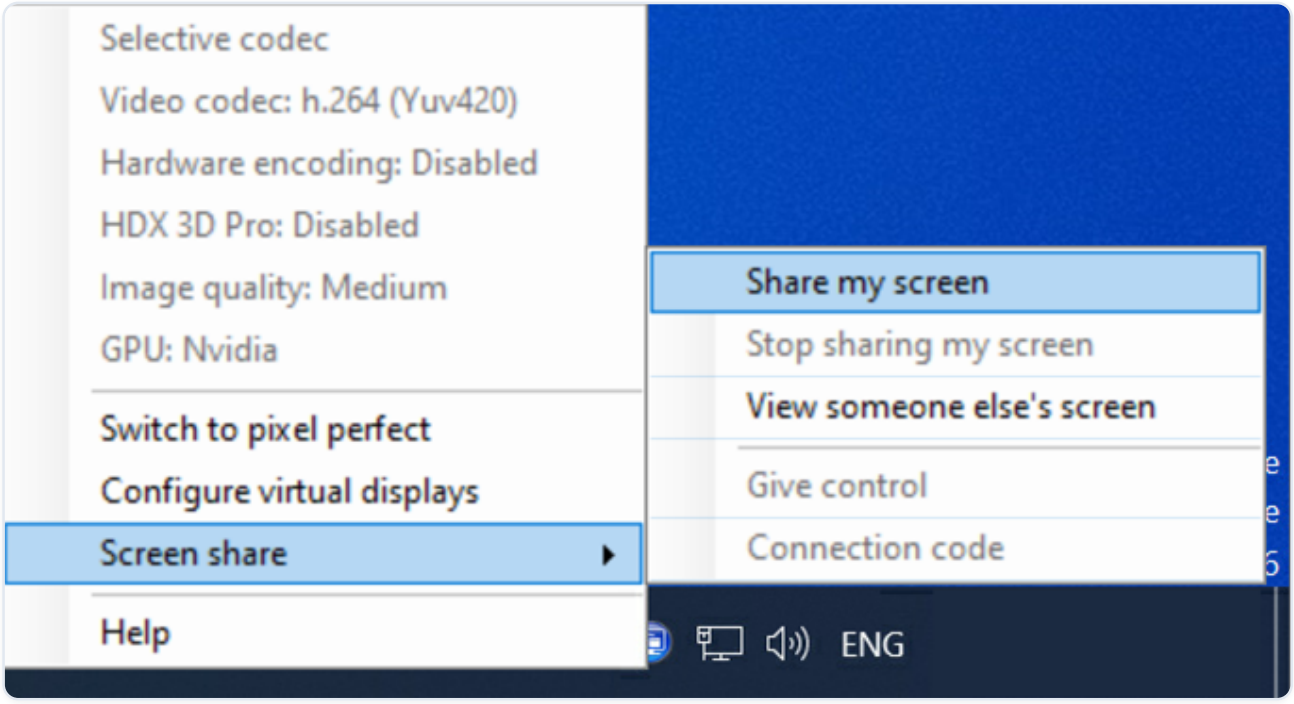
Configuração

O compartilhamento de tela deve ser habilitado usando políticas Citrix. O compartilhamento de tela é desabilitado por padrão. Configure a política de compartilhamento de tela para habilitar ou desabilitar a função e atribuir o intervalo de portas de rede utilizáveis.

Habilite a política de indicador de status gráfico para exibir a interface do usuário que inclui controles para compartilhar e conectar-se a sessões.

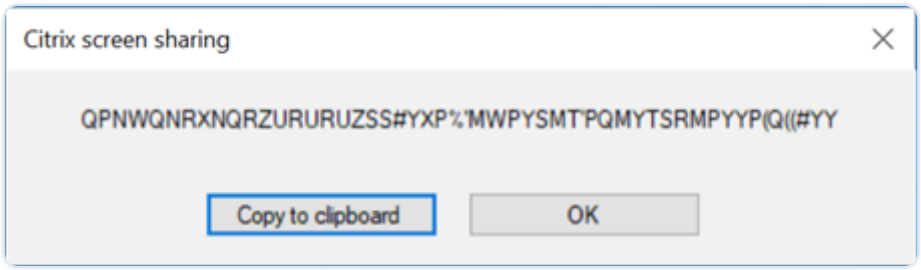
Compartilhando uma sessão

Para compartilhar uma sessão, procure o ícone do indicador de status gráfico HDX™ na área de notificação do Windows. Clique com o botão direito do mouse para exibir o menu e selecione **Compartilhar tela > Compartilhar minha tela**.



Clique em **Copiar para a área de transferência** ou selecione e copie manualmente toda a string mostrada na caixa de diálogo. A string pode então ser colada no aplicativo de sua escolha, como um cliente de e-mail ou IM, para ser distribuída a outros usuários.

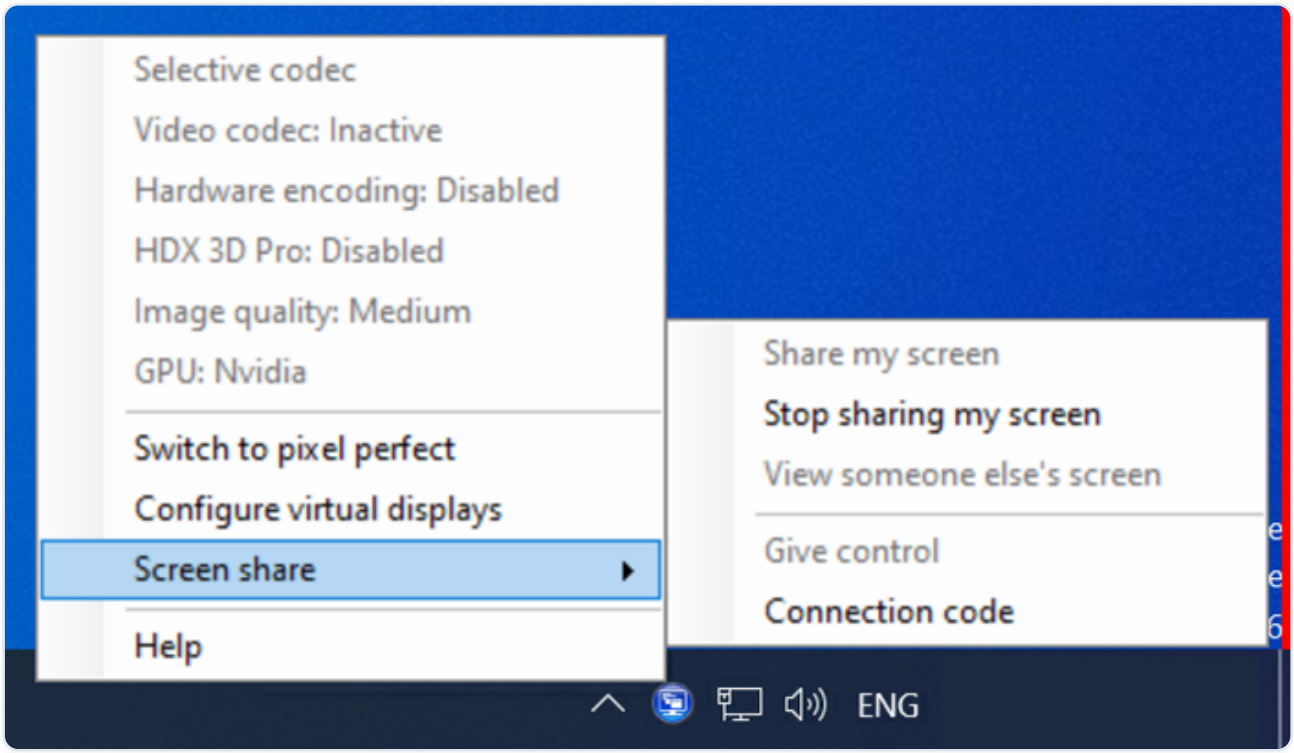
Clique em **OK** ou no **x** para fechar a caixa de diálogo. O código de conexão pode ser recuperado da opção de menu **Compartilhar tela > Código de conexão** a qualquer momento enquanto a sessão estiver sendo compartilhada.



Um contorno vermelho aparece ao redor da tela como um indicador de que a sessão está sendo compartilhada e é visível para outros.

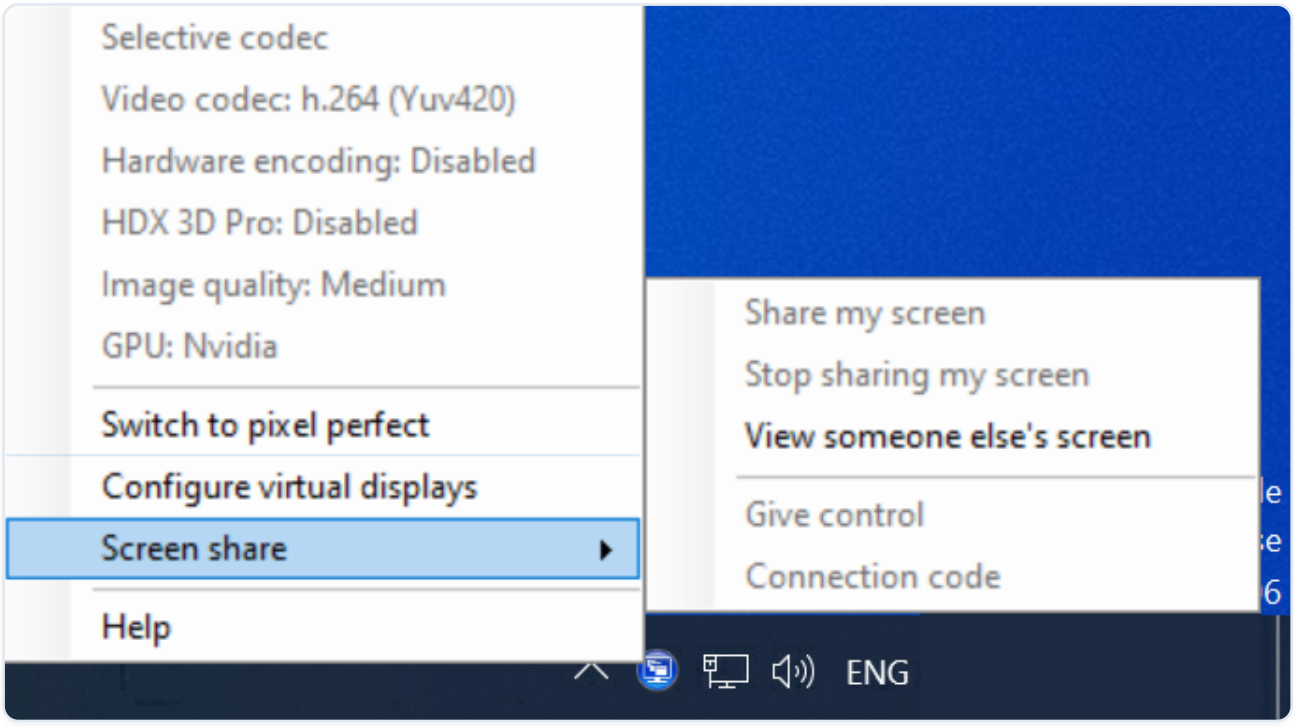
Os controles de teclado e mouse também podem ser compartilhados com outros usuários usando a opção de menu **Compartilhar tela > Conceder controle**.

Use a opção de menu **Compartilhamento de tela > Parar de compartilhar minha tela** para parar de compartilhar a sessão e desconectar todos os usuários.

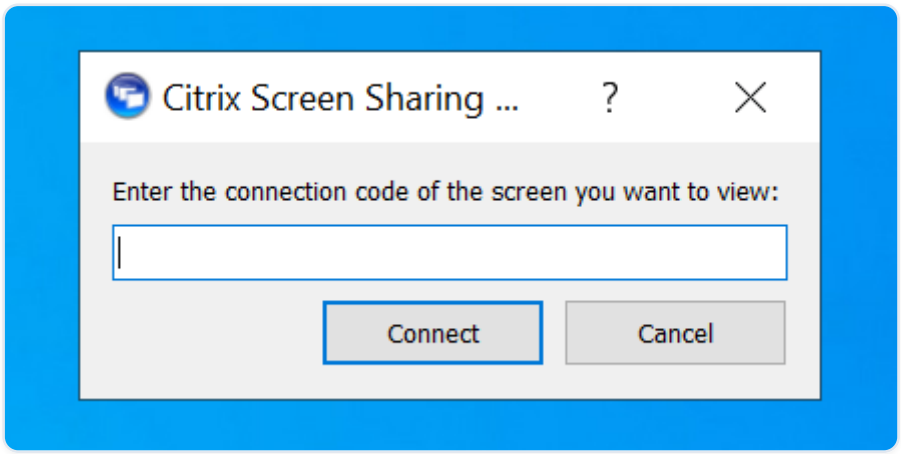


Conectando-se a uma sessão compartilhada

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 do mouse nele para exibir o menu e selecione **Compartilhamento de tela > Visualizar a tela de outra pessoa**.

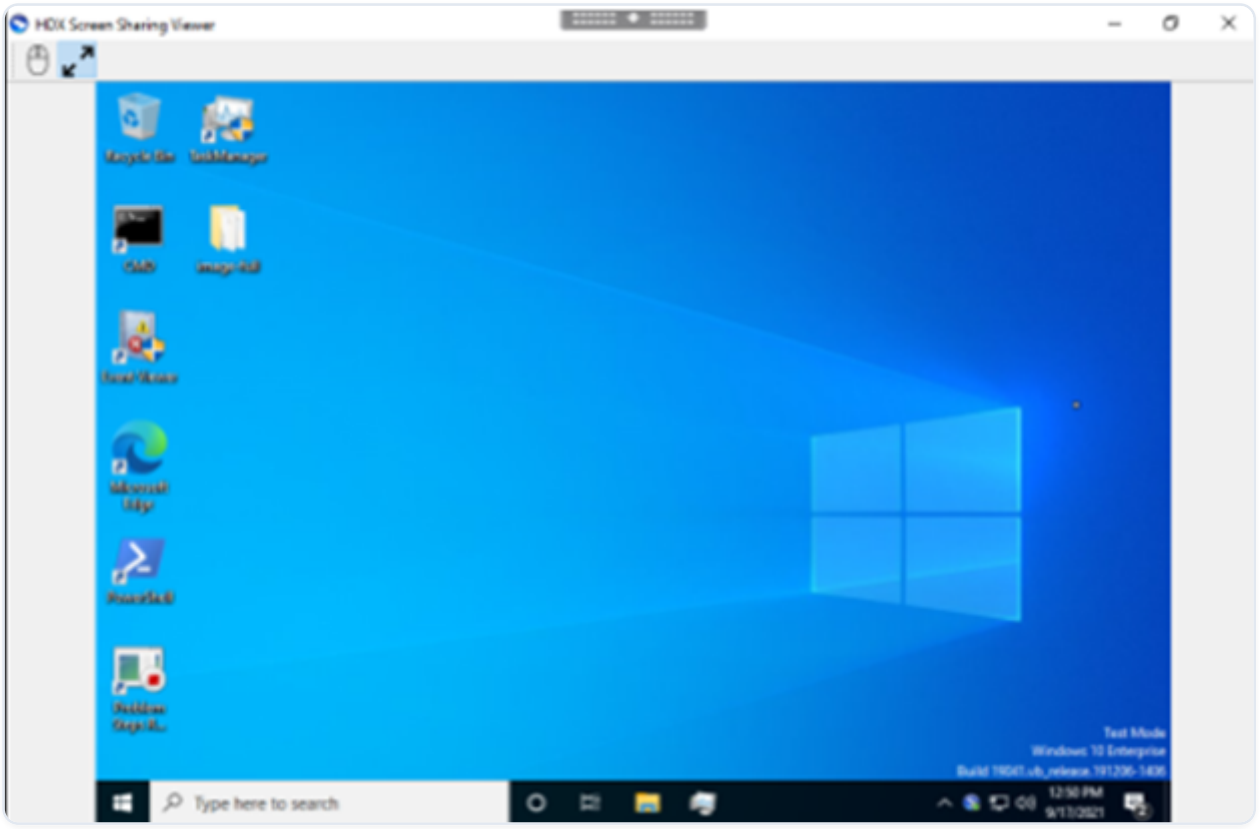


Insira ou cole a string de conexão fornecida pelo usuário que está compartilhando a sessão na caixa de texto. Clique em **Conectar** para estabelecer a conexão.



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 uma área de trabalho 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. Você não pode selecionar monitores individuais.
- O codec de vídeo H.265 não é compatível.

Multimídia

A pilha de tecnologia HDX™ oferece suporte à entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia com renderização no lado do servidor
- Redirecionamento de multimídia com renderização no lado do cliente

Essa estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, enquanto maximiza a escalabilidade do servidor para reduzir o custo por usuário.

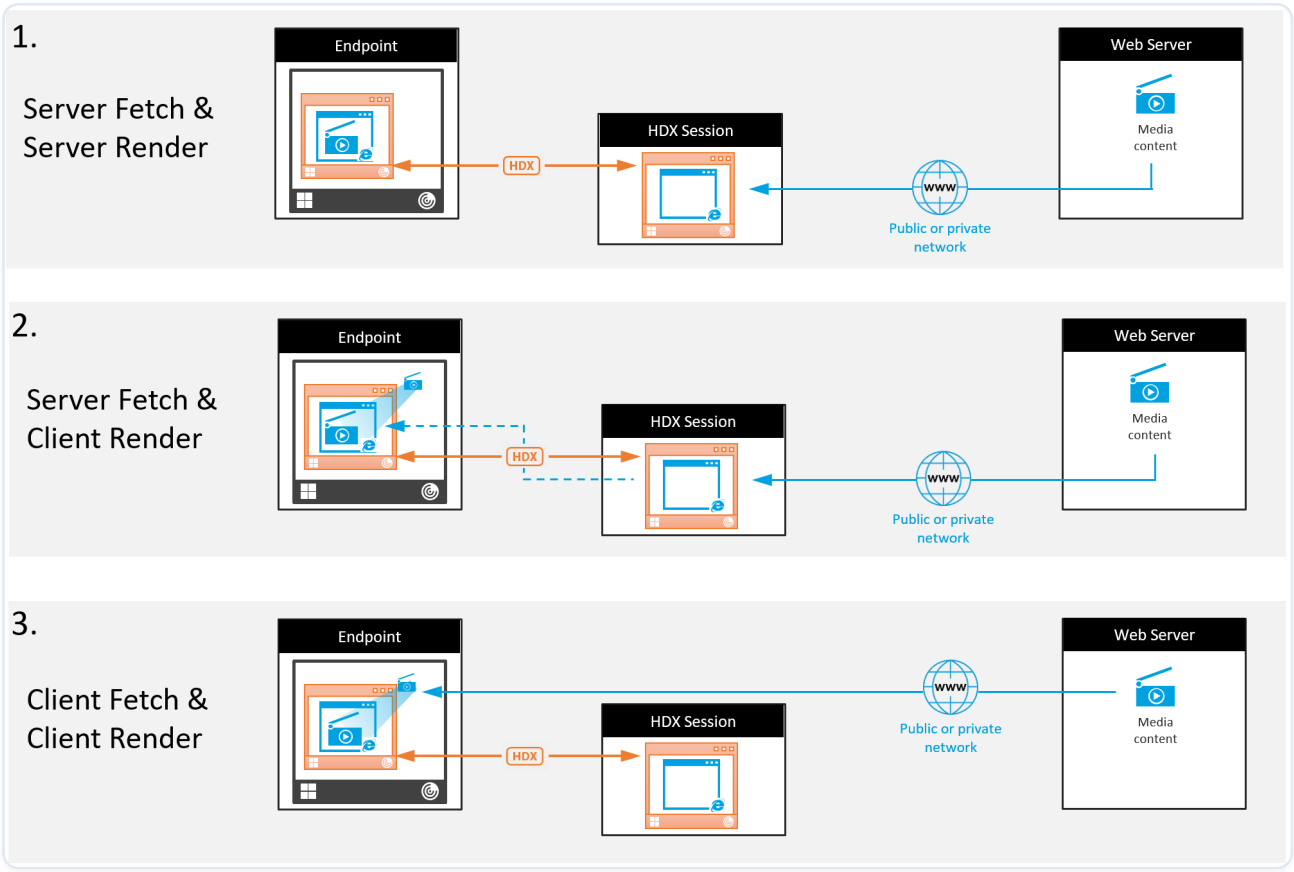
Com a entrega de multimídia renderizada no servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor Citrix Virtual Apps and Desktops pelo aplicativo. O conteúdo é então compactado e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo exige muitos recursos computacionais, a entrega de multimídia renderizada no servidor se beneficia muito da aceleração de hardware integrada. Por exemplo, o suporte para DirectX Video Acceleration (DXVA) descarrega a CPU realizando a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

Como a maioria dos servidores não oferece nenhuma aceleração de hardware para compactação de vídeo, a escalabilidade do servidor é impactada negativamente se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter alta escalabilidade do servidor, redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

- O redirecionamento do Windows Media descarrega o servidor para uma ampla variedade de formatos de mídia tipicamente associados ao Windows Media Player.
- O vídeo HTML5 tornou-se popular, e a Citrix® introduziu uma tecnologia de redirecionamento para esse tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento, como redirecionamento Host-to-client e Acesso a Aplicativos Locais, ao conteúdo multimídia.

Juntando essas tecnologias, se você não configurar o redirecionamento, o HDX fará a Renderização no Lado do Servidor. Se você configurar o redirecionamento, o HDX usará a Busca no Servidor e Renderização no Cliente ou a Busca no Cliente e Renderização no Cliente. Se esses métodos falharem, o HDX retornará à Renderização no Lado do Servidor conforme necessário e estará sujeito à Política de Prevenção de Fallback.

Cenários de exemplo



Cenário 1. (Busca no Servidor e Renderização no Servidor):

1. O servidor busca o arquivo de mídia de sua origem, decodifica e, em seguida, apresenta o conteúdo a um dispositivo de áudio ou dispositivo de exibição.
2. O servidor extrai a imagem ou som apresentado do dispositivo de exibição ou dispositivo de áudio, respectivamente.
3. O servidor opcionalmente o compacta e, em seguida, o transmite para o cliente.

Essa abordagem acarreta um alto custo de CPU, alto custo de largura de banda (se a imagem/som extraído não for compactado de forma eficiente) e tem baixa escalabilidade do servidor.

Os canais virtuais Thinwire e Áudio manipular essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para os clientes. Usando essa abordagem, a

decodificação acontece no servidor e funciona para uma variedade maior de dispositivos e formatos.

Cenário 2. (Busca pelo Servidor e Renderização pelo Cliente):

Essa abordagem depende da capacidade de interceptar o conteúdo de mídia antes que ele seja decodificado e apresentado ao dispositivo de áudio ou exibição. O conteúdo de áudio/vídeo compactado é enviado ao cliente, onde é decodificado e apresentado localmente. A vantagem dessa abordagem é que as tarefas são descarregadas para os dispositivos cliente, economizando ciclos de CPU no servidor.

No entanto, 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 ele seja buscado da fonte. 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 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 obsoletos de compactação de áudio 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:**
>
> Recomendamos a entrega de áudio usando o User Datagram Protocol (UDP) em vez de TCP quando aplicativos de áudio em tempo real são necessários. Somente o Windows Virtual Delivery Agent (VDA) oferece suporte a áudio sobre UDP.
>
> A criptografia de áudio UDP usando DTLS está disponível apenas entre o Citrix Gateway e o aplicativo Citrix Workspace™. Portanto, às vezes pode ser preferível usar o transporte TCP.

> O TCP oferece suporte à criptografia TLS de ponta a ponta do VDA para o aplicativo Citrix Workspace™.

> Para obter mais informações sobre áudio adaptável e áudio UDP, consulte Áudio sobre transporte em tempo real UDP e intervalo de porta UDP de áudio.

Qualidade do áudio

Em geral, uma qualidade de som mais alta consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para os dispositivos do usuário. A compressão de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações de política do Citrix para configurar os níveis de compressão a serem aplicados aos arquivos de som.

Por padrão, a configuração da **política de qualidade de áudio** é definida como Alta - áudio de alta definição quando o transporte TCP é usado. A política é definida como Média - otimizada para fala quando o transporte UDP (recomendado) é usado. A configuração de **áudio de alta definição** fornece áudio estéreo de alta fidelidade, mas consome mais largura de banda do que outras configurações de qualidade. Não use esta qualidade de áudio para aplicativos de chat de voz ou vídeo não otimizados (como softphones). A razão é que isso pode introduzir latência no caminho do áudio que não é adequada para comunicações em tempo real. Recomendamos a configuração de política otimizada para fala para áudio em tempo real, independentemente do protocolo de transporte selecionado.

Quando a largura de banda é limitada, por exemplo, conexões via satélite ou discadas, reduzir a qualidade do áudio para **Baixa** consome a menor largura de banda possível. Nesta situação, crie políticas separadas para usuários em conexões de baixa largura de banda para que os usuários em conexões de alta largura de banda não sejam afetados negativamente.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Diretrizes de largura de banda para reprodução e gravação de áudio:

- 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 coloca uma carga extra nos servidores e na rede. No entanto, proibir o redirecionamento de áudio do cliente desativa toda a funcionalidade de áudio HDX™.

Para obter detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Redirecionamento de microfone do cliente

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Redirecionamento de microfone do cliente** em seu padrão (Permitido).

Por segurança, os dispositivos do usuário alertam seus usuários quando servidores em que não confiam tentam acessar microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar este alerta no aplicativo Citrix Workspace.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Plug N Play de áudio

A configuração de política Plug N Play de áudio permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração está **Habilitada** por padrão. O Plug N Play de áudio permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até depois do início da sessão do usuário.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Para obter detalhes da configuração, consulte Configurações de política de áudio.

Limite de largura de banda de redirecionamento de áudio e porcentagem de limite de largura de banda de redirecionamento de áudio

A configuração de política Limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para reprodução e gravação de áudio em uma sessão.

A configuração Porcentagem de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima para redirecionamento de áudio como uma porcentagem da largura de banda total disponível.

Por padrão, zero (sem máximo) é especificado para ambas as configurações. Se ambas as configurações forem configuradas, a que tiver o menor limite de largura de banda será usada.

Para obter detalhes da configuração, consulte Configurações de política de largura de banda. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre transporte em tempo real UDP e intervalo de porta UDP de áudio

Por padrão, o Áudio sobre Transporte em Tempo Real do Protocolo de Datagrama de Usuário (UDP) é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam Áudio sobre Transporte em Tempo Real UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar UDP/RTP para áudio para garantir a melhor experiência possível ao usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio UDP é preferível ao EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que nenhuma latência seja adicionada em conexões com alta perda de pacotes.

Importante:

Quando o Citrix Gateway não está no caminho, os dados de áudio transmitidos com UDP não são criptografados. Se o Citrix Gateway estiver configurado para acessar recursos do Citrix Virtual Apps and Desktops™, o tráfego de áudio entre o dispositivo de endpoint e o Citrix Gateway é protegido usando o protocolo DTLS.

O intervalo de portas UDP de áudio especifica o intervalo de números de porta que o VDA do Windows usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é de 16500 a 16509.

Observação:

Se o transporte em tempo real de áudio sobre UDP não for necessário para áudio adaptável, a Citrix recomenda configurar a política para Desabilitado. Isso ajuda a evitar que os clientes do Citrix Workspace app solicitem conexões UDP abertas ou acionem o aparecimento de janelas de diálogo de configuração de firewall indesejadas do cliente do Citrix Workspace app.

Para obter detalhes de configuração sobre Áudio sobre UDP Real-time Transport, consulte Configurações de política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações de política de conexões multi-stream. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre UDP requer o VDA do Windows. Para políticas suportadas no VDA do Linux, consulte Lista de suporte de políticas.

Políticas de configuração de áudio para dispositivos de usuário

1. Carregue os modelos de política de grupo seguindo Configurando o modelo administrativo do Objeto de Política de Grupo.
2. No Editor de Política de Grupo, expanda **Modelos Administrativos > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Para **Configurações de áudio do cliente**, selecione **Não Configurado**, **Habilitado** ou **Desabilitado**.
    - **Não Configurado**. Por padrão, o Redirecionamento de Áudio é habilitado usando áudio de alta qualidade ou as configurações de áudio personalizadas configuradas anteriormente.
    - **Habilitado**. Habilita o redirecionamento de áudio usando as opções selecionadas.
    - **Desabilitado**. Desabilita o redirecionamento de áudio.
4. Se você selecionar **Habilitado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Habilitar Transporte em Tempo Real** e então defina o intervalo de portas de entrada a serem abertas no firewall local do Windows.
6. Para usar Áudio UDP com Citrix Gateway, selecione **Permitir Transporte em Tempo Real Através do gateway**. Configure o Citrix Gateway com DTLS. Para mais informações, consulte este artigo.

Como Administrador, se você não tiver controle sobre os dispositivos de endpoint para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o Áudio UDP. Por exemplo, para dispositivos pessoais ou computadores domésticos.

1. Na máquina StoreFront, abra C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica com um editor como o notepad.
2. Faça as seguintes entradas na seção .

    ; Este texto habilita o Transporte em Tempo Real

    EnableRtpAudio=true

    ; Este texto permite o Transporte em Tempo Real Através do gateway

    EnableUDPThroughGateway=true

```
; Este texto define a qualidade do áudio como Média

AudioBandwidthLimit=1

; Intervalo de portas UDP

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

Se você habilitar o áudio do User Datagram Protocol (UDP) editando default.ica, o áudio UDP será habilitado para todos os usuários que estiverem usando essa loja.

Evitar eco durante conferências multimídia

Usuários em conferências de áudio ou vídeo podem ouvir um eco. Ecos geralmente ocorrem quando alto-falantes e microfones estão muito próximos um do outro. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX oferece uma opção de cancelamento de eco (habilitada por padrão) que minimiza qualquer eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Certifique-se de que os dispositivos não estejam muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração do registro para desabilitar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados por meio do registro.

Softphones

Um softphone é um software que atua como uma interface de telefone. Você usa um softphone para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Ao usar um softphone, você pode discar números de telefone e realizar outras funções relacionadas ao telefone usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para a entrega de softphones.

- **Modo de controle**. O softphone hospedado controla um aparelho telefônico físico. Neste modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.

- **Suporte a softphone otimizado para HDX RealTime (recomendado)**. O mecanismo de mídia é executado no dispositivo do usuário, e o tráfego de Voz sobre Protocolo de Internet flui de ponto a ponto. Para exemplos, consulte:
  - Otimização HDX para Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone para VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings para VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin VDI do Zoom
  - Genesys PureEngage Cloud
  - Dispositivo de ditado Nuance Dragon PowerMic
- **Acesso a aplicativos locais**. Um recurso do Citrix Virtual Apps and Desktops que permite que um aplicativo, como um softphone, seja executado localmente no dispositivo de usuário Windows, mas apareça perfeitamente integrado ao seu desktop virtual/publicado. Esse recurso descarrega todo o processamento de áudio para o dispositivo do usuário. Para obter mais informações, consulte Acesso a aplicativos locais e redirecionamento de URL.
- **Suporte genérico a softphone HDX RealTime.** Voz sobre Protocolo de Internet sobre ICA.

Suporte genérico a softphone

O suporte genérico a softphone permite hospedar um softphone não modificado no XenApp ou XenDesktop no datacenter. O tráfego de áudio passa pelo protocolo Citrix ICA (preferencialmente usando UDP/RTP) para o dispositivo do usuário que executa o aplicativo Citrix Workspace.

O suporte genérico a softphone é um recurso do HDX RealTime. Essa abordagem para entrega de softphone é especialmente útil quando:

- Uma solução otimizada para entregar o softphone não está disponível e o usuário não está em um dispositivo Windows onde o Acesso a Aplicativos Locais possa ser usado.
- O mecanismo de mídia necessário para a entrega otimizada do softphone não está instalado no dispositivo do usuário ou não está disponível para a versão do sistema operacional em execução no dispositivo do usuário. Nesse cenário, o HDX RealTime Genérico fornece uma solução de fallback valiosa.

Existem duas considerações sobre a entrega de softphone usando Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é entregue ao desktop virtual/publicado.
- Como o áudio é entregue para e do headset, microfone e alto-falantes do usuário, ou conjunto de telefone USB.

Citrix Virtual Apps and Desktops incluem inúmeras tecnologias para suportar a entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida do áudio em tempo real e eficiência de largura de banda.
- Pilha de áudio de baixa latência.
- Buffer de jitter do lado do servidor para suavizar o áudio quando a latência da rede flutua.
- Marcação de pacotes (DSCP e WMM) para Qualidade de Serviço.
    - Marcação DSCP para pacotes RTP (Camada 3)
    - Marcação WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voz sobre Protocolo de Internet. O aplicativo Citrix Workspace para Windows oferece estes recursos:

- Buffer de jitter do lado do cliente - Garante áudio suave mesmo quando a latência da rede flutua.
- Cancelamento de eco - Permite maior variação na distância entre o microfone e os alto-falantes para trabalhadores que não usam fone de ouvido.
- Áudio plug-n-play - Dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.
- Roteamento de dispositivo de áudio - Os usuários podem direcionar o toque para os alto-falantes, mas o caminho de voz para o fone de ouvido.
- ICA multi-stream - Permite roteamento flexível baseado em Qualidade de Serviço pela rede.
- O ICA suporta quatro fluxos TCP e dois UDP. Um dos fluxos UDP suporta o áudio em tempo real sobre RTP.

Para um resumo dos recursos do aplicativo Citrix Workspace, consulte Matriz de Recursos do Citrix Receiver.

Recomendações de configuração do sistema

Hardware e Software do Cliente: Para uma qualidade de áudio ideal, recomendamos a versão mais recente do aplicativo Citrix Workspace e um fone de ouvido de boa qualidade que tenha cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac suportam Voz sobre Protocolo de Internet. Além disso, a Dell Wyse oferece suporte a Voz sobre Protocolo de Internet para ThinOS (WTOS).

Considerações sobre a CPU: Monitore o uso da CPU no VDA para determinar se é necessário atribuir duas CPUs virtuais a cada máquina virtual. Voz e vídeo em tempo real são intensivos em dados. A configuração de duas CPUs virtuais reduz a latência de troca de threads. Portanto, recomendamos que você configure duas vCPUs em um ambiente VDI do Citrix Virtual Desktops™.

Ter duas CPUs virtuais não significa necessariamente dobrar o número de CPUs físicas, pois as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de Confiabilidade da Sessão, também aumenta o consumo de CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo de CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor poderoso.

Áudio UDP: O áudio sobre UDP oferece excelente tolerância a congestionamento de rede e perda de pacotes. Recomendamos usá-lo em vez de TCP quando disponível.

Configuração de LAN/WAN: A configuração adequada da rede é fundamental para uma boa qualidade de áudio em tempo real. Normalmente, você deve configurar redes locais virtuais (VLANs) porque pacotes de broadcast excessivos podem introduzir jitter. Dispositivos habilitados para IPv6 podem gerar muitos pacotes de broadcast. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configure para suportar Qualidade de Serviço.

Configurações para uso de conexões WAN: Você pode usar bate-papo por voz em conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se estiver entregando softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler® SD-WAN entre o data center e o escritório remoto. Isso mantém uma alta Qualidade de Serviço. O NetScaler SD-WAN suporta ICA Multi-Stream, incluindo UDP. Além disso, para um único fluxo TCP, é possível distinguir as prioridades de vários canais virtuais ICA para garantir que os dados de áudio em tempo real de alta prioridade recebam tratamento preferencial.

Use o Director ou o HDX Monitor para validar sua configuração HDX.

Conexões de usuário remoto: O Citrix Gateway suporta DTLS para entregar tráfego UDP/RTP nativamente (sem encapsulamento em TCP). Abra os firewalls bidirecionalmente para tráfego UDP na Porta 443.

Seleção de codec e consumo de largura de banda: Entre o dispositivo do usuário e o VDA no data center, recomendamos usar a configuração de codec **Otimizado para Fala**, também conhecida como áudio de Qualidade Média. Entre a plataforma VDA e o IP-PBX, o softphone usa qualquer codec configurado ou negociado. Por exemplo:

- G711 oferece boa qualidade de voz, mas tem um requisito de largura de banda de 80 kilobits por segundo a 100 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).
- G729 oferece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo a 40 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).

Entrega de aplicativos de softphone para o desktop virtual

Existem dois métodos pelos quais você pode entregar um softphone para o desktop virtual XenDesktop®:

- O aplicativo pode ser instalado na imagem do desktop virtual.
- O aplicativo pode ser transmitido por streaming para o desktop virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciamento porque a imagem do desktop virtual é mantida organizada. Após ser transmitido por streaming para o desktop virtual, o aplicativo é executado nesse ambiente como se tivesse sido instalado da maneira usual. Nem todos os aplicativos são compatíveis com o App-V.

Entrega de áudio para e do dispositivo do usuário

O HDX RealTime genérico suporta dois métodos de entrega de áudio para e do dispositivo do usuário:

- **Canal Virtual de Áudio Citrix**. Geralmente recomendamos o Canal Virtual de Áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB Genérico**. Suporta dispositivos de áudio com botões ou um display (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou similar à LAN de volta para o servidor Citrix Virtual Apps and Desktops.

Canal virtual de áudio Citrix

O Canal Virtual de Áudio Bidirecional da 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 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 um tempo de codificação rápido e consome apenas aproximadamente 56 Kilobits por segundo de largura de banda de rede (28 Kbps em cada direção), no pico. Este codec deve ser explicitamente selecionado no console do Studio porque não é o codec de áudio padrão. O padrão é o codec de áudio HD (Alta Qualidade). Este codec é excelente para trilhas sonoras estéreo de alta fidelidade, mas é mais lento para codificar em comparação com o codec Otimizado para Fala.

Redirecionamento USB Genérico

A tecnologia de Redirecionamento USB Genérico da Citrix (canal virtual CTXGUSB) fornece um meio genérico de acesso remoto a dispositivos USB, incluindo dispositivos compostos (áudio mais HID) e dispositivos USB isócronos. Essa abordagem é limitada a usuários conectados à LAN. A razão é que o protocolo USB tende a ser sensível à latência da rede e requer uma largura de banda considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones. Este redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o Canal Virtual de Áudio Citrix é preferido porque é otimizado para tráfego de áudio. A principal exceção é quando você está usando um dispositivo de áudio com botões. Por exemplo, um telefone USB conectado ao dispositivo do usuário que está conectado à LAN do data center. Neste caso, o Redirecionamento USB Genérico suporta botões no aparelho telefônico ou headset que controlam recursos enviando um sinal de volta para o softphone. Não há problema com botões que funcionam localmente no dispositivo.

Limitação

Você instala um dispositivo de áudio no seu cliente, habilita o redirecionamento de áudio e inicia uma sessão RDS. Os arquivos de áudio podem falhar ao reproduzir e uma mensagem de erro aparece.

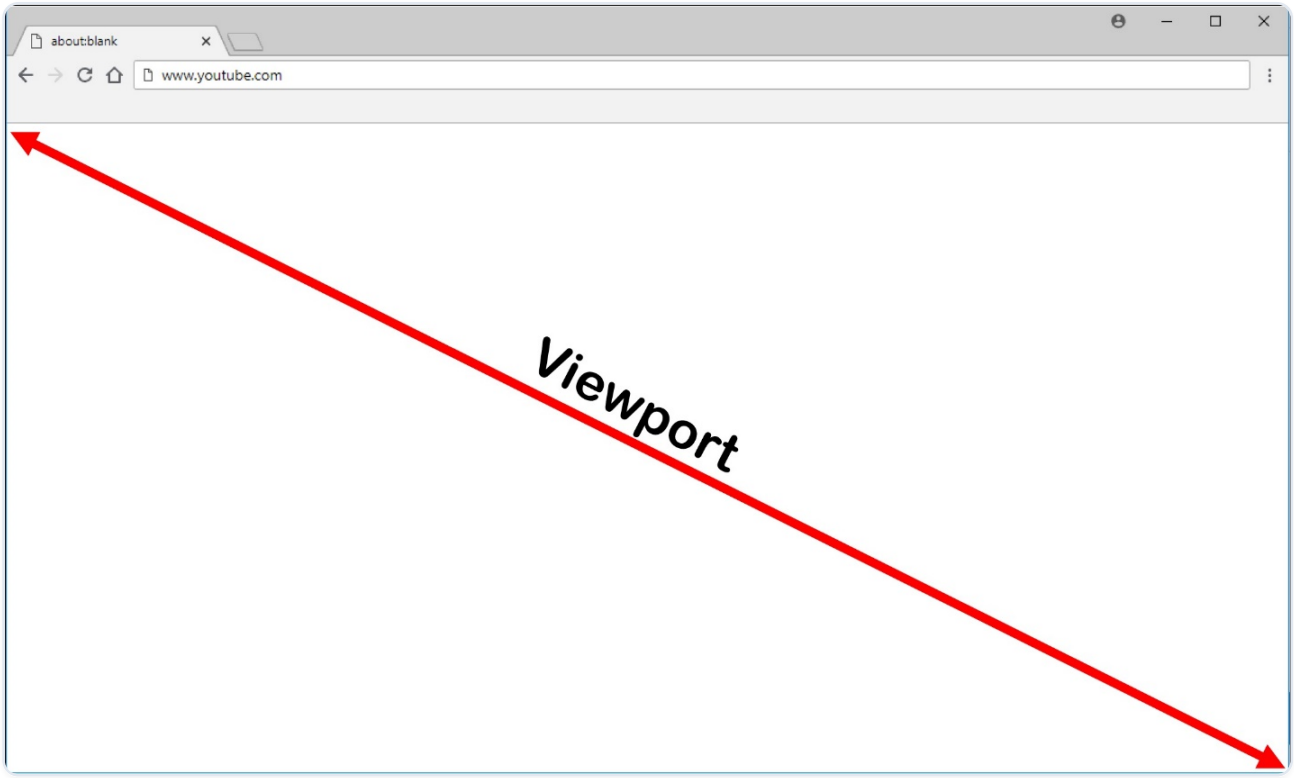
Como solução alternativa, adicione a chave do Registro na máquina RDS e, em seguida, reinicie a máquina. Para obter informações, consulte Limitação de áudio na lista de recursos gerenciados por meio do Registro.

Redirecionamento de conteúdo do navegador

O redirecionamento de conteúdo do navegador impede a renderização de páginas da web na lista de permissões no lado do VDA. Esse recurso usa o aplicativo Citrix Workspace™ para Windows ou o aplicativo Citrix Workspace para Linux para instanciar um mecanismo de renderização correspondente no lado do cliente, que busca o conteúdo HTTP e HTTPS da URL.

> **Observação:**
>
> Você pode especificar que as páginas da web sejam redirecionadas para o lado do VDA (e não redirecionadas no lado do cliente) usando uma lista de bloqueio.
>
> Este mecanismo de layout da web de sobreposição é executado no dispositivo de endpoint em vez de no VDA e usa a CPU, GPU, RAM e rede do endpoint.

Apenas a área de visualização do navegador é redirecionada. A área de visualização é a área retangular no seu navegador onde o conteúdo é exibido. A área de visualização não inclui itens como a Barra de Endereços, Barra de Ferramentas de **Favoritos**, Barra de Status. Esses itens estão na interface do usuário, que ainda estão sendo executados no navegador no VDA.



1. Configure uma política do Studio que especifique uma Lista de Controle de Acesso contendo as URLs na lista de permissões para redirecionamento ou a lista de bloqueio que desabilita o

redirecionamento para caminhos de URL específicos. Para que o navegador no VDA detecte que a URL para a qual o usuário está navegando corresponde à lista de permissões ou não corresponde a uma lista de bloqueio, uma extensão do navegador realiza a comparação. A extensão do navegador para o Internet Explorer 11 está incluída na mídia de instalação e é instalada automaticamente. Para o Chrome, a extensão do navegador está disponível na Chrome Web Store, e você pode implantá-la usando as Políticas de Grupo e arquivos ADMX. As extensões do Chrome são instaladas por usuário. A atualização de uma imagem dourada para adicionar ou remover uma extensão não é necessária.

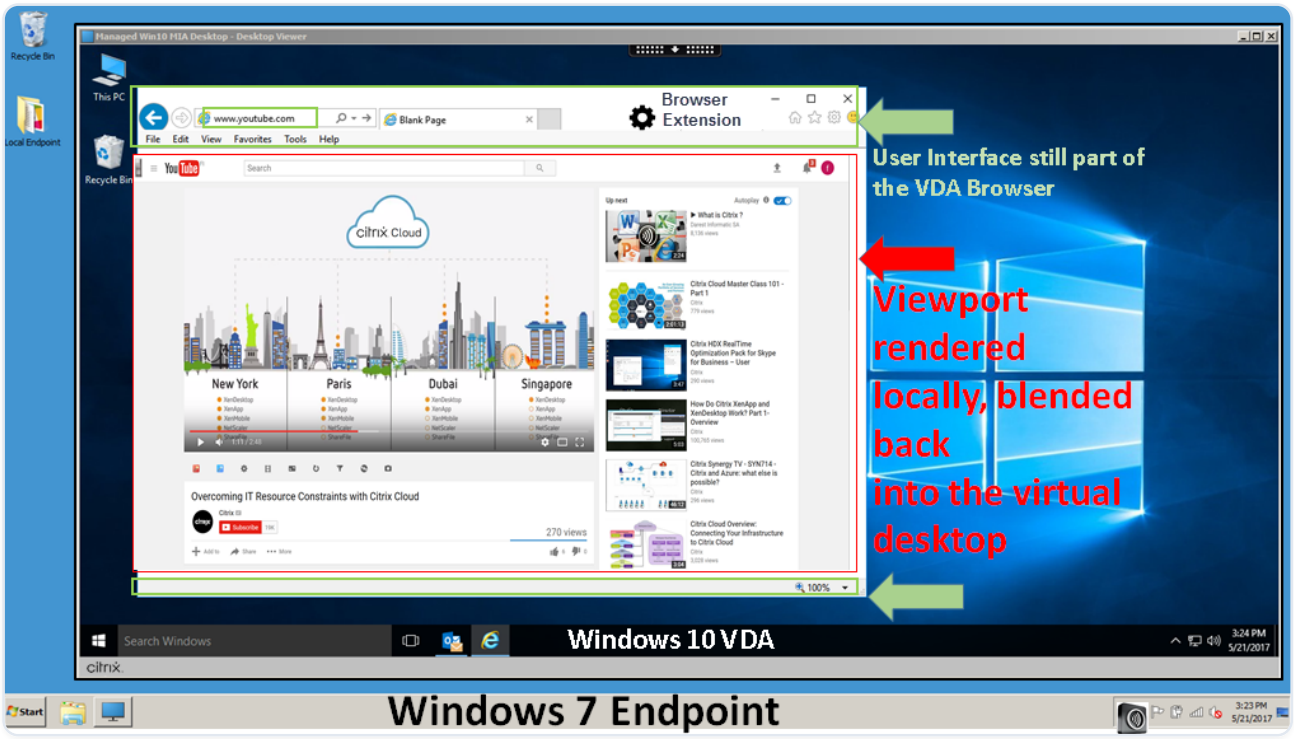
2. Se uma correspondência for encontrada na lista de permissões (por exemplo `https://www.mycompany.com/`), e não houver correspondência com uma URL na lista de bloqueio (por exemplo `https://www.mycompany.com/engineering`), um canal virtual (CTXCSB) instrui o aplicativo Citrix Workspace de que um redirecionamento é necessário e retransmite a URL. O aplicativo Citrix Workspace então instancia um mecanismo de renderização local e exibe o site.
3. O aplicativo Citrix Workspace então integra o site de volta à área de conteúdo do navegador da área de trabalho virtual de forma transparente.

> **Observação:**
>
> Para obter mais informações sobre as novidades e correções para a extensão de redirecionamento de conteúdo do navegador, vá para a Chrome Web Store e pesquise "citrix® bcr" para encontrar a extensão.

> A cor do logotipo especifica o status da extensão do Chrome. É uma destas três cores:

- Verde: Ativo e conectado.
- Cinza: Não ativo/ocioso na guia atual.
- Vermelho: Quebrado/Não funcionando.

Você pode depurar o registro usando **Opções** no menu de extensões.



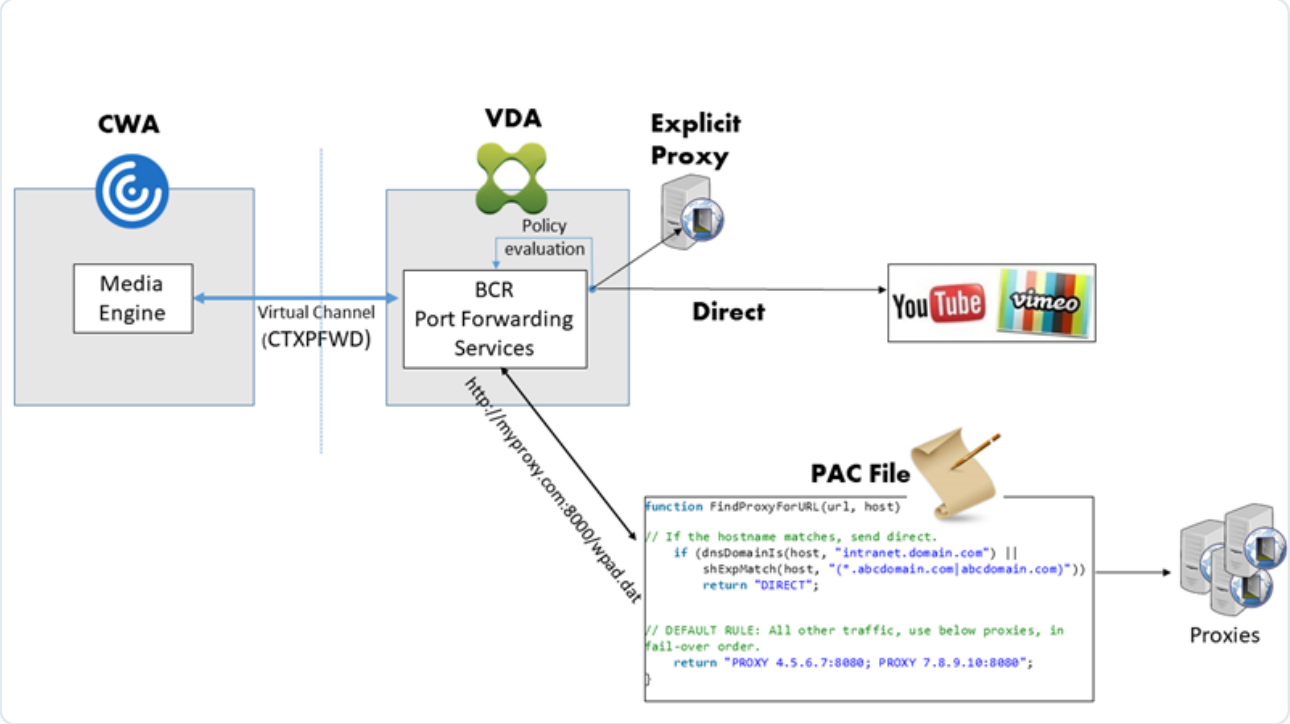
Aqui estão os cenários de como o aplicativo Citrix Workspace busca conteúdo:

- **Busca no servidor e renderização no servidor**: Não há redirecionamento porque você não adicionou o site à lista de permissões ou o redirecionamento falhou. Voltamos a renderizar a página da web no VDA e usamos o Thinwire para remotar os gráficos. Use políticas para controlar o comportamento de fallback. Alto consumo de CPU, RAM e largura de banda no VDA.
- **Busca no servidor e renderização no cliente**: O aplicativo Citrix Workspace contata e busca conteúdo do servidor web através do VDA usando um canal virtual (CTXPFWD). Esta opção é útil quando o cliente não tem acesso à internet (por exemplo, thin clients). Baixo consumo de CPU e RAM no VDA, mas a largura de banda é consumida no canal virtual ICA®.

  Existem três modos de operação para este cenário. O termo proxy refere-se a um dispositivo proxy que o VDA acessa para obter acesso à Internet.

  Qual opção de política escolher:

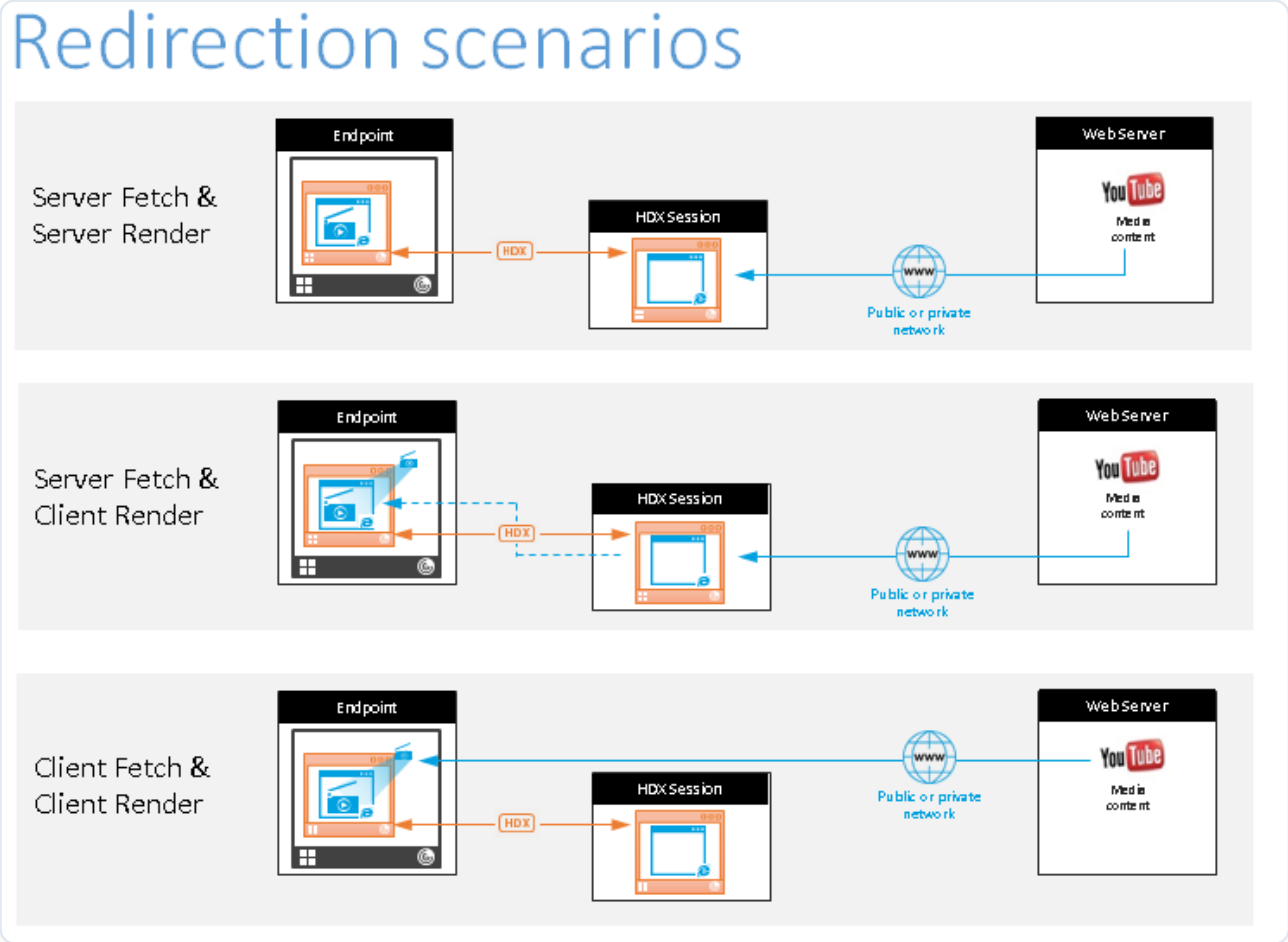
  - Proxy Explícito - Se você tiver um único proxy explícito em seu data center.
  - Direto ou Transparente - Se você não tiver proxies, ou se usar proxies transparentes.
  - Arquivos PAC - Se você depende de arquivos PAC para que os navegadores no VDA possam escolher automaticamente o servidor proxy apropriado para buscar uma URL especificada.



- **Busca no cliente e renderização no cliente**: Como o aplicativo Citrix Workspace contata o servidor web diretamente, ele requer acesso à internet. Este cenário descarrega todo o uso de rede, CPU e RAM do seu Site XenApp e XenDesktop®.

  Benefícios:

  - Melhor experiência do usuário final (Taxa de Bits Adaptativa (ABR))
  - Uso reduzido de recursos do VDA (CPU/RAM/E/S)
  - Consumo reduzido de largura de banda



Mecanismo de fallback:

Pode haver momentos em que o redirecionamento do cliente falhe. Por exemplo, se a máquina cliente não tiver acesso direto à internet, uma resposta de erro pode ser enviada de volta ao VDA. Nesses casos, o navegador no VDA pode recarregar e renderizar a página no servidor.

Você pode suprimir a renderização de elementos de vídeo no servidor usando a política existente de **prevenção de fallback do Windows Media**. Defina esta política como **Reproduzir todo o conteúdo apenas no cliente** ou **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Essas configurações impedem que elementos de vídeo sejam reproduzidos no servidor se houver falhas no redirecionamento do cliente. Esta política entra em vigor somente quando você habilita o redirecionamento de conteúdo do navegador e a política de **Lista de Controle de Acesso** contém a URL que retorna ao fallback. A URL não pode estar na política de lista de bloqueio.

Requisitos do sistema:

Endpoints Windows:

- Windows 10
- Citrix Workspace app 1809 para Windows ou posterior

> **Observação:**

> O redirecionamento de conteúdo do navegador é suportado apenas na Versão Atual do Citrix Workspace app para Windows, mas não nas versões LTSR do Citrix Workspace app, 1912 e 2203.1.

> Endpoints Linux:

- Citrix Workspace app 1808 para Linux ou posterior
- Terminais thin client devem incluir WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp and XenDesktop 7.15 CU5 ou posterior:

- Sistema operacional VDA: Windows 10 (versão mínima 1607), Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
- Navegador no VDA:
  - Google Chrome v66 ou posterior (o Chrome requer o aplicativo Citrix Workspace 1809 para Windows ou posterior no endpoint do usuário, Citrix Virtual Apps and Desktops™ 7 1808 VDA ou posterior e a extensão de redirecionamento de conteúdo do navegador)
  - Internet Explorer 11 e configure estas opções:
    - Desmarcar **Modo Protegido Aprimorado** em: **Opções da Internet** > **Avançado > Segurança**
    - Marcar **Habilitar extensões de navegador de terceiros** em: **Opções da Internet > Avançado > Navegação**

Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo da Central de Conhecimento https://support.citrix.com/article/CTX230052

Extensão do Chrome de redirecionamento de conteúdo do navegador

Para usar o redirecionamento de conteúdo do navegador com o Chrome, adicione a extensão de redirecionamento de conteúdo do navegador da Chrome Web Store. Clique em **Adicionar ao Chrome** no ambiente Citrix Virtual Apps and Desktops.

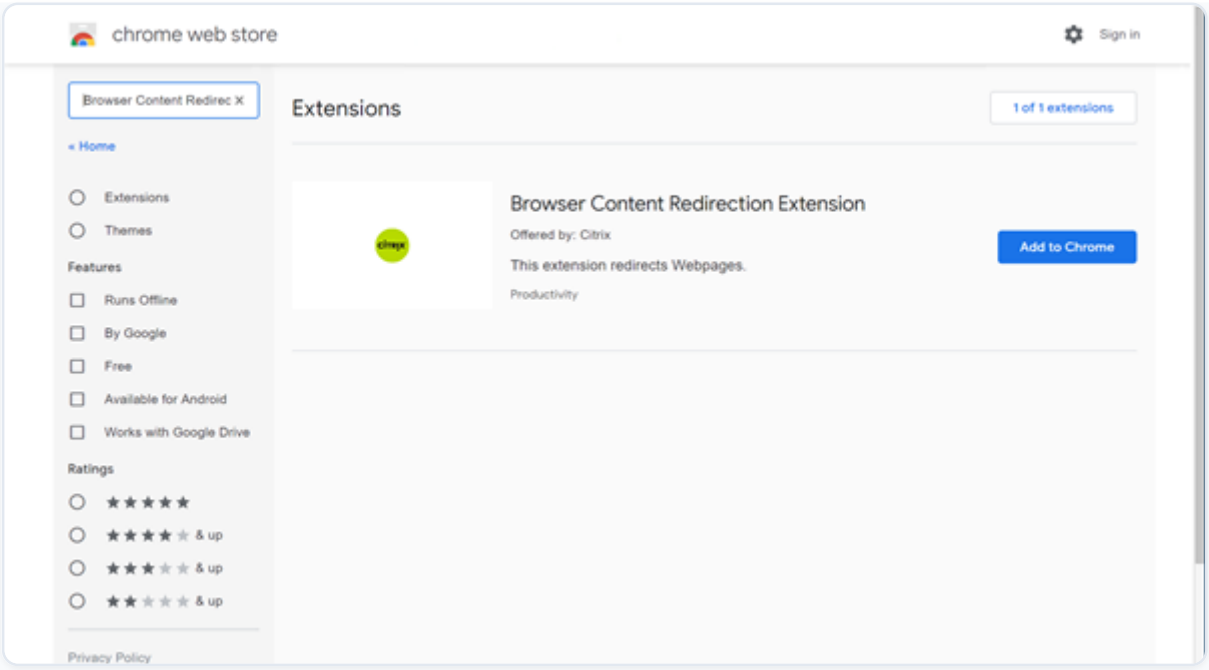
A extensão **não** é necessária na máquina cliente do usuário – apenas no VDA.

Requisitos do sistema

- Chrome v66 ou superior
- Extensão de redirecionamento de conteúdo do navegador
- Citrix Virtual Apps and Desktops 7 1808 ou superior
- Citrix Workspace app 1809 para Windows ou superior

Observação:

O redirecionamento de conteúdo do navegador é suportado apenas na Versão Atual do Citrix Workspace app para Windows, mas não nas versões LTSR do Citrix Workspace app, 1912 e 2203.1.

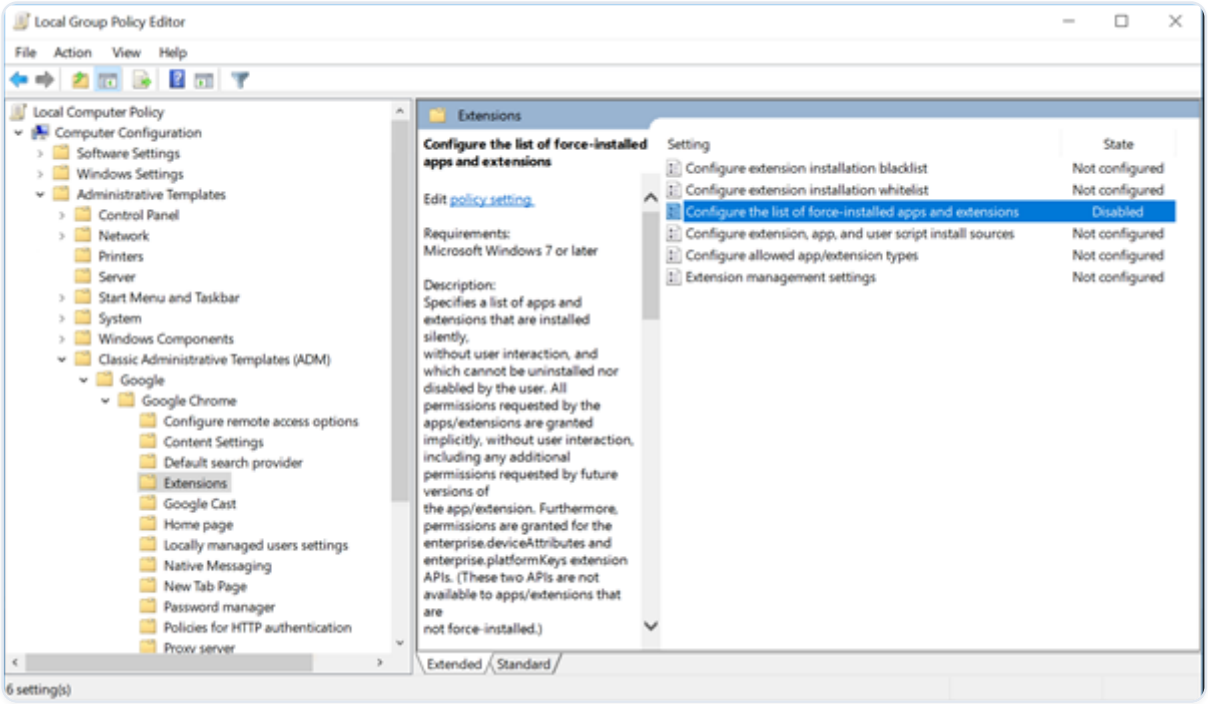


Este método funciona para usuários individuais. Para implantar a extensão para um grande grupo de usuários em sua organização, implante a extensão usando a Política de Grupo.

Implantar a extensão usando a Política de Grupo

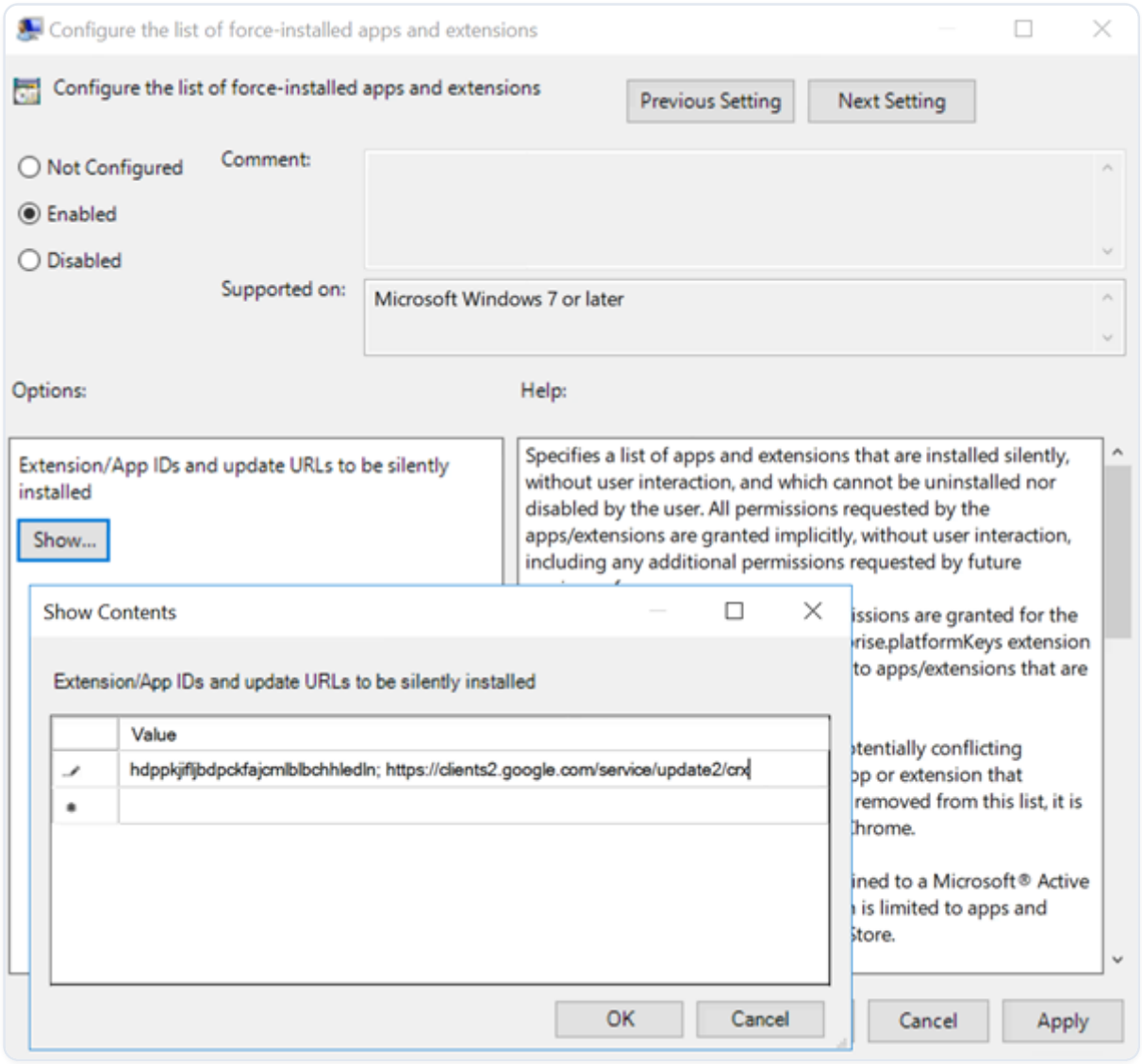
1. Importe os arquivos ADMX do Google Chrome para o seu ambiente. Para obter informações sobre como baixar modelos de política e instalar e configurar os modelos em seu Editor de Política de Grupo, consulte Definir políticas do navegador Chrome em PCs gerenciados.
2. Abra seu console de Gerenciamento de Política de Grupo e vá para **Configuração do Usuário \ Modelos Administrativos\Modelos Administrativos Clássicos (ADM) \ Google**

Google Chrome \ Extensões. Habilite a configuração **Configurar a lista de aplicativos e extensões instalados à força**.



3. Clique em **Mostrar** e digite a seguinte string, que corresponde ao ID da extensão. Atualize o URL para a extensão de redirecionamento de conteúdo do navegador.

`hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx`



4. Aplique a configuração e, após uma atualização de **gpupdate**, o usuário recebe automaticamente a extensão. Se você iniciar o navegador Chrome na sessão do usuário, a extensão já estará aplicada e ele não poderá removê-la.

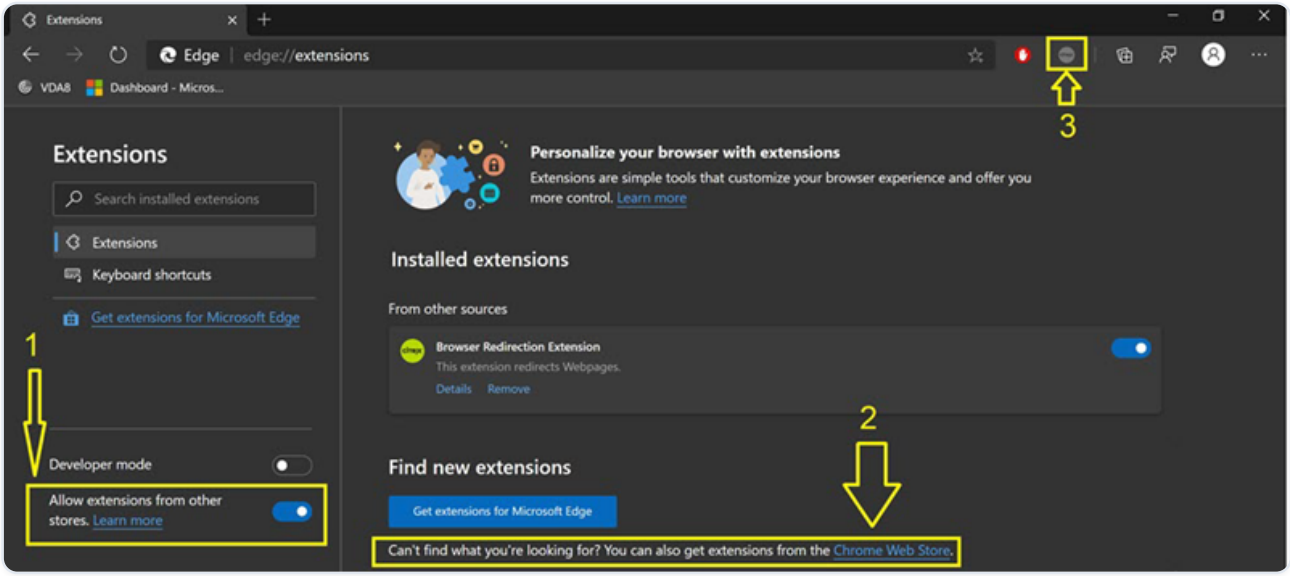
   Quaisquer atualizações da extensão são instaladas automaticamente nas máquinas dos usuários por meio do URL de atualização que você especificou na configuração.

   Se a configuração **Configurar a lista de aplicativos e extensões instalados à força** estiver definida como **Desativada**, a extensão será automaticamente removida do Chrome para todos os usuários.

Extensão do Edge Chromium para redirecionamento de conteúdo do navegador

Para instalar a extensão de redirecionamento de conteúdo do navegador no Edge, certifique-se de ter a versão **83.0.478.37** ou superior do navegador Edge instalada.

1. Clique na opção **Extensões**. Escolha **Gerenciar extensão**. Ative **Permitir extensões de outras lojas**.
2. Clique no link da **Chrome Web Store** e a extensão aparecerá na barra superior direita. Para obter mais informações sobre as extensões do Microsoft Edge, consulte Extensões.



Redirecionamento de conteúdo do navegador e DPI

Ao usar o redirecionamento de conteúdo do navegador com o DPI (escala) definido para qualquer valor acima de 100% na máquina do usuário, a tela de conteúdo do navegador redirecionado é exibida incorretamente. Para evitar esse problema, não defina o DPI ao usar o redirecionamento de conteúdo do navegador. Outra maneira de evitar o problema é desabilitar a aceleração de GPU do redirecionamento de conteúdo do navegador para o Chrome, criando a chave de registro na máquina do usuário. Para obter informações, consulte Redirecionamento de conteúdo do navegador e DPI na lista de recursos gerenciados por meio do registro.

Logon único com Autenticação Integrada do Windows

A redireção de conteúdo do navegador aprimora a sobreposição para usar o esquema Negotiate para autenticação em servidores web configurados com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA.

Por padrão, a redireção de conteúdo do navegador usa um esquema de autenticação básico que exige que os usuários autenticar com suas credenciais VDA cada vez que acessam o servidor web. Para logon único, você pode habilitar a configuração de política **Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador** ou criar uma chave de registro no VDA.

Antes de habilitar o logon único, conclua o seguinte:

- Configure a infraestrutura Kerberos para emitir tickets para nomes de entidade de serviço (SPNs) construídos a partir do nome do host. Por exemplo, `HTTP/serverhostname.com`.
- Para busca no servidor: Ao usar a redireção de conteúdo do navegador no modo de busca no servidor, certifique-se de que o DNS esteja configurado corretamente no VDA.
- Para busca no cliente: Ao usar a redireção de conteúdo do navegador no modo de busca no cliente, certifique-se de que o DNS esteja configurado corretamente no dispositivo cliente e que você permita conexões TCP da sobreposição para o endereço IP do servidor web.

Para configurar o logon único usando a política de redirecionamento de conteúdo do navegador, consulte a configuração Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador.

Alternativamente, você pode habilitar o logon único em um servidor web adicionando uma chave de registro no VDA. Para obter informações, consulte Logon único com Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador na lista de recursos gerenciados através do registro.

Cabeçalho de solicitação User-agent

O cabeçalho user-agent ajuda a identificar as solicitações HTTP enviadas da redireção de conteúdo do navegador. Essa configuração pode ser útil ao configurar regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas da redireção de conteúdo do navegador, você pode criar uma regra que contenha o cabeçalho user-agent para ignorar certos requisitos.

Somente dispositivos Windows suportam o cabeçalho de solicitação de user-agent.

Por padrão, a string do cabeçalho de solicitação user-agent está desabilitada. Para habilitar o cabeçalho user-agent para conteúdo renderizado pelo cliente, use o editor de Registro. Para obter informações, consulte Cabeçalho de solicitação User-agent na lista de recursos gerenciados através do registro.

Compatibilidade do cliente de redirecionamento de conteúdo do navegador

Você pode usar o WMI para verificar se seu cliente é compatível com a redireção de conteúdo do navegador. Qualquer método para acessar o WMI funciona. O seguinte é um exemplo usando PowerShell.

1. Abra o PowerShell.
2. Execute `Get-WmiObject -Class CTXBCRStatus`.

3. Verifique o parâmetro `BCR_Capable`.
    - Se `True`, o cliente é compatível com o redirecionamento de conteúdo do navegador.
    - Se `False`, o cliente não é compatível com o redirecionamento de conteúdo do navegador.

Informações adicionais

- Se `CtxBrowserSvc` não estiver disponível, nenhum resultado será exibido ao executar o comando.
- Se `CtxBrowserSvc` nunca foi executado, os resultados retornam um erro de classe inválida.

Conferência de vídeo 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**.

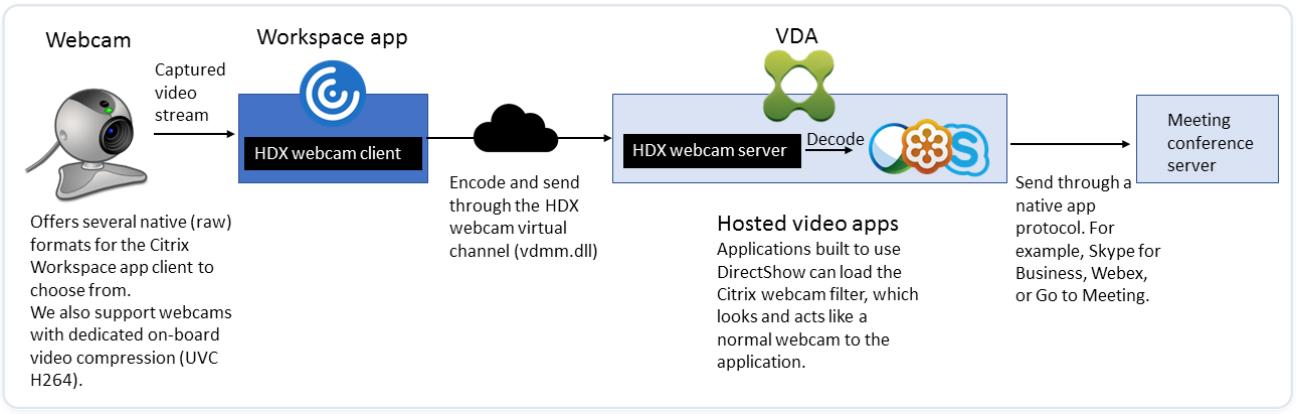
Compactação de vídeo de webcam HDX

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 estrutura multimídia que faz parte do sistema operacional cliente para interceptar vídeo de dispositivos de captura, transcodificá-lo e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do SO.

O cliente lida com a comunicação com a webcam. O cliente então envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua integração oferece a mesma experiência em sua área de trabalho. O aplicativo Workspace compacta o vídeo para economizar largura de banda e fornecer melhor resiliência em cenários de WAN.



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

- Conferência multimídia
- Redirecionamento de Mídia do Windows

Se uma webcam suportar codificação de hardware, a compactação de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de

banda do que a codificação de software. Para forçar a compactação de software, edite a chave do Registro no cliente. Para obter informações, consulte Compactação de software de webcam na lista de recursos gerenciados por meio do Registro.

Requisitos de compactação de vídeo de webcam HDX

A compactação de vídeo de webcam HDX suporta as seguintes versões do Citrix Workspace app:

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 e 64 bits no XenApp e XenDesktop 7.17 e posteriores. 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 posteriores. Em versões anteriores, o aplicativo Citrix Workspace para Mac oferece suporte apenas a aplicativos de 32 bits.
Aplicativo Citrix Workspace para Linux	O aplicativo Citrix Workspace para Linux oferece suporte apenas a aplicativos de 32 bits na área de trabalho virtual.
Aplicativo Citrix Workspace para Chrome	Como alguns Chromebooks ARM não oferecem suporte à codificação H.264, apenas aplicativos de 32 bits podem usar a 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 ou superior. Para obter mais informações, consulte o artigo do Knowledge Center CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.

- Webcam compatível com DirectShow (use as configurações padrão da webcam). Webcams com capacidade de codificação de hardware reduzem o uso da CPU no 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 upstream. A Citrix usa as seguintes webcams para a validação inicial do recurso:

- Modelos Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- Webcam HP Deluxe

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 resoluções de webcam de até 1920x1080.

Este recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver para Windows, versão mínima 4.10.

Você pode usar uma chave 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 padrão de 352x288 CIF. 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 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 de multimídia HTML5 estende os recursos de redirecionamento de multimídia do HDX™ MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento da 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 os plug-ins proprietários, incluindo:

- Padrões independentes de empresas (W3C)
- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança levantados pelos plug-ins

Downloads progressivos HTTP

O download progressivo HTTP é um método de pseudo-streaming baseado em HTTP que suporta HTML5. Em um download progressivo, o navegador reproduz um único arquivo (codificado em uma única qualidade) enquanto ele está sendo baixado de um servidor web HTTP. O vídeo é armazenado na unidade à medida que é recebido e é reproduzido a partir da unidade. Se você assistir ao vídeo novamente, o navegador pode carregar o vídeo do cache.

Para um exemplo de download progressivo, consulte a página de teste de redirecionamento de vídeo HTML5. Para inspecionar os elementos de vídeo na página da web e encontrar as fontes (formato de contêiner mp4) nas tags de vídeo HTML5, use as ferramentas de desenvolvedor em seu navegador:

Comparando HTML5 e Flash

RECURSO	HTML5	FLASH
Requer um player proprietário	Não	Sim
Funciona 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.

Oferecemos suporte ao seguinte e usamos políticas para controlá-los. Para obter mais informações, consulte Configurações de política de multimídia.

- Renderização do lado do servidor

- Renderização do cliente com busca do servidor
- Busca e renderização do lado do cliente

Versões mínimas do aplicativo Citrix Workspace™ e do Citrix Receiver™:

- Aplicativo Citrix Workspace 1808 para Windows
- Citrix Receiver para Windows 4.5
- Aplicativo Citrix Workspace 1808 para Linux
- Citrix Receiver para Linux 13.5

VERSÃO MÍNIMA DO NAVEGADOR VDA	VERSÃO/COMPILAÇÃO/SP DO 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 confiáveis 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** - 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: **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

- Para a entidade final (folha): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) Localização: **Certificates (Local Computer) > Personal > Certificates**.

- **WebSocketService.exe** - Executa no sistema local e realiza a terminação SSL e o mapeamento da sessão do usuário. WebSocket Seguro TLS escutando na porta 9001 de 127.0.0.1.
- **WebSocketAgent.exe** - Executa na sessão do usuário e renderiza o vídeo conforme instruído pelos comandos do WebSocketService.

Como faço para habilitar o redirecionamento de vídeo HTML5?

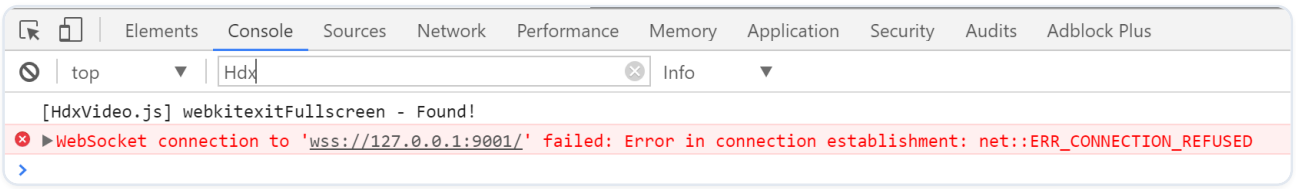
Nesta versão, este recurso está disponível apenas para páginas web controladas. Requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de Taxa de Bits Adaptativa (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não são suportados.

Para obter mais informações, consulte *Configurações de política de multimídia*.

Dicas de Solução de Problemas

Podem ocorrer erros quando a página web tenta executar o HdxVideo.js. Se o JavaScript falhar ao carregar, o mecanismo de redirecionamento HTML5 falha. Certifique-se de que não há erros relacionados ao HdxVideo.js inspecionando o console nas janelas da ferramenta de desenvolvedor do seu navegador. Por exemplo:



Otimização para Microsoft Teams (Clássico)

A Citrix oferece otimização para Microsoft Teams baseado em desktop usando Citrix Virtual Apps and Desktops™ e o aplicativo Citrix Workspace™. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

Nossa otimização para Microsoft Teams inclui serviços HDX™ do lado do VDA e uma API para interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O endpoint decodifica e fornece o multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem nativamente no aplicativo hospedado do Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um canal virtual de comando e controle. Isso significa que a mídia não é trocada entre o aplicativo Citrix Workspace e o VDA.

Apenas client-fetch/client-render está disponível.

Esta demonstração em vídeo lhe dá uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam a versão mais recente disponível do Microsoft Teams e que ela seja mantida atualizada. As versões do aplicativo de desktop do Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas. As versões não suportadas do aplicativo de desktop do Microsoft Teams exibem uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Teams (Desktop e Mac).

> **Nota:**
>
> Recomendamos instalar o VDA antes de instalar o Microsoft Teams na imagem dourada. Essa ordem de instalação é necessária para que o sinalizador **ALLUSER=1** entre em vigor. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA, desinstale e reinstale o Microsoft Teams. Se você estiver usando o App Layering, consulte Para App Layering para obter mais detalhes.

> Recomendamos que você siga as diretrizes de instalação do Microsoft Teams em toda a máquina. Além disso, evite usar o instalador .exe que instala o Microsoft Teams em `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador **ALLUSER=1** na linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

Este exemplo também usa o parâmetro **ALLUSERS=1**. Ao definir esse 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 é atualizado automaticamente sempre que há uma nova versão. Recomendamos este modo para ambientes não persistentes, como aplicativos ou desktops compartilhados hospedados em um servidor Windows ou catálogos aleatórios/agrupados do Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação VDI).

Suponha que você tenha ambientes VDI persistentes dedicados do Windows 10. Você deseja que o aplicativo Microsoft Teams 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**.

Para Acesso Remoto a PC

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior após a instalação do VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 e posteriores incluem lógica aumentada executada no momento do lançamento do Microsoft Teams e no momento do login para detecção do VDA. Essas versões também incluem identificação do tipo de sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, versões anteriores do Microsoft Teams podem falhar ao detectar e desabilitar certos recursos ou elementos da interface do usuário. Por exemplo, Salas de Reunião, janelas pop-out para reuniões e bate-papo, ou reações de reunião.

Em alguns cenários de Acesso Remoto a PC, ao reconectar-se a uma sessão anteriormente não otimizada a partir de um novo endpoint que oferece suporte à otimização HDX, pode ser necessário reiniciar o Microsoft Teams para oferecer suporte à otimização HDX.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, implante esta chave de registro em VDAs do Windows antes de instalar o Microsoft Teams com **ALLUSER=1**. Para obter informações, consulte Otimização para Microsoft Teams com Citrix App Layering na lista de recursos gerenciados por meio do registro.

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 de máquina ampla), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**

> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> Um logon de usuário subsequente aciona a instalação final em **AppData**.

Instalador para toda a máquina

A seguir, um exemplo de pastas, atalhos da área de trabalho e registros criados pela instalação do instalador para toda a máquina do Microsoft Teams em uma VM Windows Server 2016 de 64 bits:

Pasta:

- `C:\Program Files (x86)\Microsoft\Teams`

- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho da Área de Trabalho:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registro:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`
- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> O local do registro varia de acordo com os Sistemas Operacionais subjacentes e a arquitetura (bitness).

Recomendações

- Recomendamos desativar a inicialização automática excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do seu dia de trabalho) aumentem o uso da CPU da VM.
- Se a área de trabalho virtual não tiver uma GPU/vGPU, recomendamos definir **Desativar aceleração de hardware da GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada em `%Appdata%\Microsoft\Teams` em `desktop-config.json`. Você pode usar um script de logon para editar esse arquivo e definir o valor como **true**.
- Se estiver usando o Citrix Workspace Environment Management™ (WEM), ative a **Proteção contra Picos de CPU** para gerenciar o consumo do processador para o Microsoft Teams.

Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação difere. Todos os arquivos são colocados em AppData.

Pasta:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho na área de trabalho:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

Registro:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Melhores Práticas

As recomendações de melhores práticas são baseadas nos cenários de caso de uso. Usar o Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente dos dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as informações específicas do usuário apropriadas são armazenadas em cache durante a sessão do usuário. Por exemplo, as informações específicas do usuário incluem dados do usuário, perfil e configurações. Sincronize os dados nestas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Lista de exclusão de conteúdo em cache do Microsoft Teams para configuração não persistente

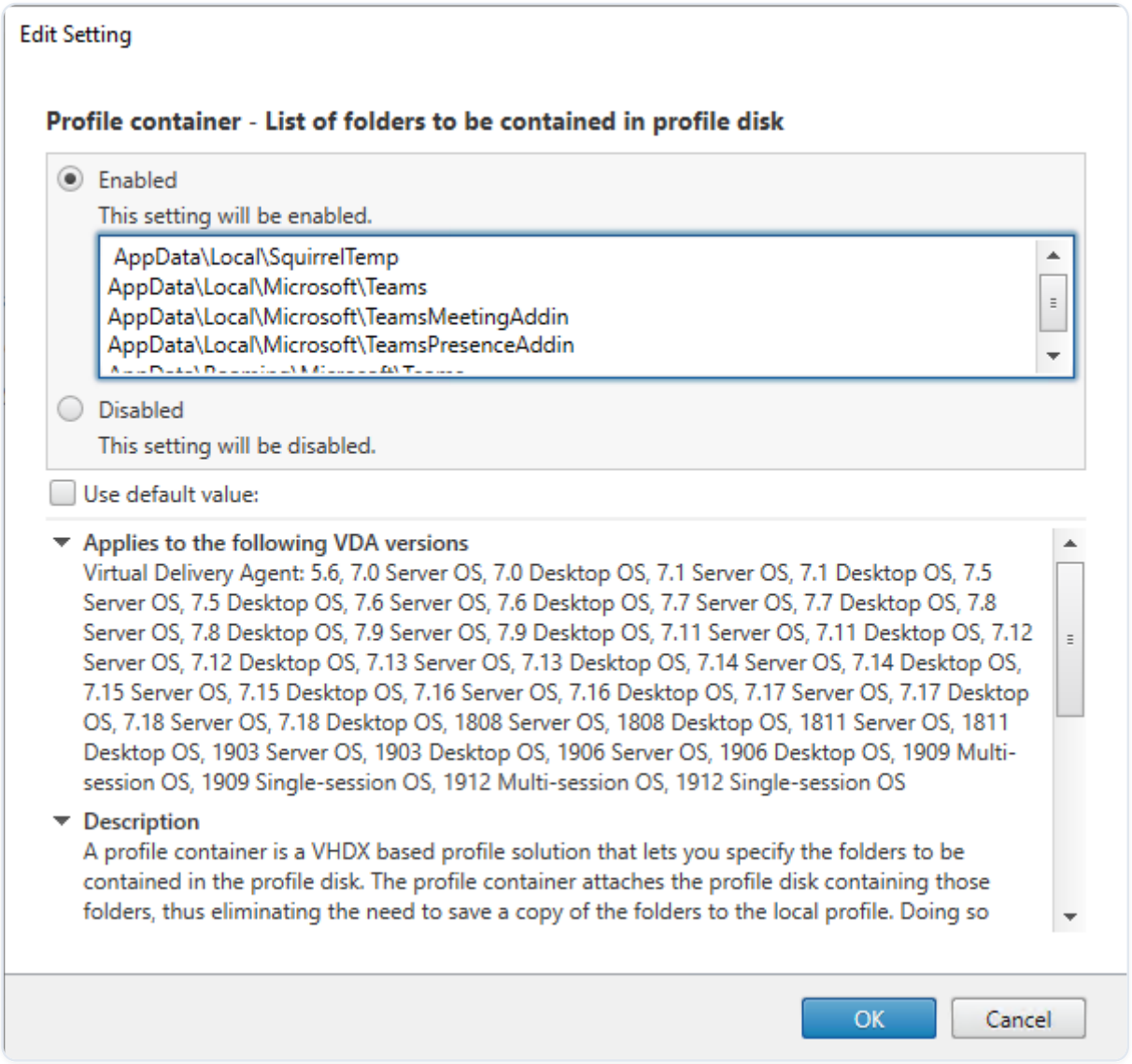
Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams conforme descrito na documentação Microsoft. Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais sua configuração não persistente.

Caso de uso: cenário de sessão única

Nesse cenário, o usuário final usa o Microsoft Teams em um local por vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop, e o Microsoft Teams é implantado no desktop virtual como um aplicativo. Recomendamos habilitar o contêiner

de perfil do Citrix e redirecionar os diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador do Microsoft Teams para toda a máquina (**ALLUSER=1**) na imagem dourada.
2. Habilite o Citrix Profile Management e configure o armazenamento de perfil de usuário com as permissões adequadas.
3. Habilite a seguinte configuração de política do Profile Management: **Sistema de arquivos > Sincronização > Contêiner de perfil – Lista de pastas a serem contidas no disco de perfil**.



Liste todos os diretórios por usuário nesta configuração. Você também pode configurar essas definições usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplicar as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

Requisitos do sistema

Versão mínima recomendada - Delivery Controller (DDCs) 1906.2

Se você estiver usando uma versão anterior, consulte Habilitar otimização do Microsoft Teams:

Sistemas operacionais suportados:

- Windows Server 2022, 2019, 2016, 2012R2 Standard e edições de data center, e com a opção Server Core

Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais suportados:

- Windows 11.
- Windows 10 de 64 bits, versões 1607 e posteriores. Aplicativos hospedados em VM são suportados no Citrix Workspace app para Windows 2109.1 e posterior.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edições Standard e data center).

Requisitos:

- BCR_x64.msi - o MSI que inclui o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não o exclua.

Versão recomendada – Citrix Workspace app para Windows CR mais recente e Versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 e 64 bits, incluindo edições Embedded) (O suporte para Windows 7 foi interrompido na Versão 2006) (O suporte para Windows 8.1 foi interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas de processador (CPU) suportadas: x86 e x64 (ARM não é suportado).
- Requisito de endpoint: CPU dual core de aproximadamente 2,2–2,4 GHz que pode suportar resolução HD de 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs dual ou quad-core com velocidades base mais baixas (~1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Thin Clients HP verificados: t630/t640, t730/t740, mt44/mt45.

- Thin Clients Dell verificados: 5070, 5470 Mobile TC e AIO.
- Thin Clients 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de endpoints verificados, consulte Thin Clients.
- O aplicativo Citrix Workspace requer pelo menos 600 MB de espaço livre em disco e 1 GB de RAM.
- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se ele não estiver presente no sistema.

Os administradores podem habilitar/desabilitar o Microsoft Teams iniciando no modo otimizado alterando a política de otimização do Teams. Os usuários que iniciam no modo otimizado no aplicativo Citrix Workspace não podem desabilitar o Microsoft Teams.

Versão mínima - aplicativo Citrix Workspace 2006 para Linux

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
- Distribuição Linux x64

Hardware:

- CPU dual-core de no mínimo 1,8 GHz que suporte resolução HD de 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com velocidade base de 1,8 GHz e alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de endpoints verificados, consulte Thin Clients.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desabilitar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é

VDWEBRTC=On. Após a conclusão da atualização, reinicie a Sessão. (É necessária permissão de root).

Versão mínima - aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais suportados:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e posterior.
- macOS Monterey.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Nota:**

> O aplicativo Citrix Viewer requer acesso às preferências de Segurança e Privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência em **Menu Apple > Preferências do Sistema > Segurança e Privacidade > Guia Privacidade > Gravação de tela** e selecionam **Citrix Viewer**.

> A otimização do Microsoft Teams funciona por padrão com o aplicativo Citrix Workspace 2012 e posterior e macOS 10.15.

Se você quiser desabilitar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versão mínima - Versão mais recente do aplicativo Citrix Workspace para Chrome OS executando a versão mais recente do Chrome OS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core 2.4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desabilitada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de Servidor Único

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) podem ser suportados em um único host físico. Isso é comumente referido como Escalabilidade de Servidor Único (SSS) do Citrix Virtual Apps and Desktops. No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade de usuário. A ideia é descobrir quantos usuários ou VMs podem ser executados em uma única peça de hardware executando um hypervisor principal.

> **Nota:**

> Esta seção inclui orientações para estimar o SSS. Observe que as orientações são de alto nível e podem não ser necessariamente específicas para sua situação ou ambiente exclusivo. A única maneira de realmente entender o SSS do Citrix Virtual Apps and Desktops é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda usar estas orientações e estas regras simples apenas para estimar rapidamente o SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar hardware ou tomar qualquer decisão financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2,60 GHz (Turbo máximo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- Armazenamento SSD local RAID 0 (11 discos) 6 TB

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

Terminologia

- Carga de trabalho de trabalhador do conhecimento: Inclui Acrobat Reader, Freemind/Java, Visualizador de fotos, Edge e aplicativos do MS Office, como Excel, Outlook, PowerPoint e Word.
- Linha de base: Testes de escalabilidade de servidor executados com carga de trabalho de trabalhador do conhecimento (sem Microsoft Teams).
- Carga de trabalho do Microsoft Teams: Carga de trabalho típica de trabalhador do conhecimento + Microsoft Teams.

Como o Microsoft Teams é testado sob estresse

- O Microsoft Teams é otimizado com HDX. Assim, todo o processamento multimídia é descarregado para o endpoint ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou encerrados antes do início da carga de trabalho.
- Abrir o Microsoft Teams (Inicialização a frio).
- Medir o tempo que o Microsoft Teams leva para carregar e focar na janela principal do Microsoft Teams.
- Alternar para a janela de chat usando atalhos de teclado.
- Alternar para a janela do calendário usando atalhos de teclado.
- Enviar a mensagem de chat para um usuário específico usando atalhos de teclado.
- Alternar para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- Impacto de 40% na escalabilidade com a Carga de Trabalho do Microsoft Teams (81 usuários), em comparação com a Linha de Base (137 usuários).
- Aumentar a capacidade do servidor em ~40% (em CPU) restaura o número de usuários como na carga de trabalho da Linha de Base.
- 20% de memória extra necessária com a Carga de Trabalho do Microsoft Teams, em comparação com a Linha de Base.
- Aumentar o tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% na gravação de IOPS, aumento de ~100% na leitura de IOPS. O Microsoft Teams pode ter um impacto significativo em ambientes com armazenamento mais lento.

Matriz de recursos e suporte de versão

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA WINDOWS CR	APLICATIVO CITRIX WORKSPACE PARA WINDOWS 1912 LTSR (E CU1-CU4)	APLICATIVO CITRIX WORKSPACE PARA WINDOWS 1912 CU5	APLICATIVO CITRIX WORKSPACE PARA WINDOWS 1912 CU6 (OU POSTERIOR)	APLICATIVO CITRIX WORKSPACE PARA MAC	APLICATIVO CITRIX WORKSPACE PARA LINUX	CITRIX WORKSPACE APP PARA CHROMEOS
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	Sim	Sim	Sim	2012	2006	2105.5 (1)
i. Borda vermelha do indicador de tela	Versão atual menos 90 dias	1906	2002	Sim	Sim	Sim	2012	2006	Não
ii. Limitar a captu	Versão atual meno	1906	2009.5	Não	Sim	Sim	2012	2006	Não

ra ao Desktop Viewer	s 90 dias								
iii. Vários monitores	Versão atual menos 90 dias	1906	2106 (2)	Não	Não	Sim (2)	2106	2106	Não
DTMF	Versão atual menos 90 dias	N/A	2102	Não	Sim (5)	Sim (5)	2101	2101	2111.1
Suporte a Servidor Proxy	Versão atual menos 90 dias	N/A	2012 (3)	Não	Sim (3) (5)	Sim (3) (5)	2104 (4)	2101 (4)	Não
Compartilhamento de apps	Versão atual menos 90 dias	2109	2109.1	Não	Não	Não	2203.1	Não	Não
Multi Window	1.5.0.0.11865	2112	2112.1	Não	Não	Não	2203.1	2203	Não
Conceder Controle	Versão atual meno	N/A	2112.1	Não	Não	Não	2203.1	Não	Não

	s 90 dias								
Solicitar Controle	Versão atualmenos 90 dias	N/A	2112.1	Não	Não	Não	2203.1	Não	Não
Legendas ao Vivo	Versão atualmenos 90 dias	N/A	2109.1	Não	Não	Não	2109	2109	Não
e911 Dinâmico	Versão atualmenos 90 dias	N/A	2112.1	Não	Não	Não	2112	2112	2112

1. Desativado por padrão, requer que o Administrador o ative.
2. Visualizador de CD somente em modo de tela cheia. SHIFT+F2 não é suportado.
3. Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados.
4. Somente anônimo.
5. Apenas no Windows 10, SO Cliente Windows IoT.
6. Recursos atualmente indisponíveis no Microsoft Teams. Para obter informações sobre o ETA, consulte a página Microsoft.

Habilitar otimização do Microsoft Teams

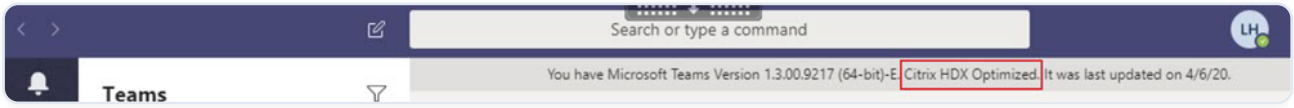
Para habilitar a otimização para o Microsoft Teams, use a política do console de gerenciamento descrita na política de redirecionamento do Microsoft Teams. Esta política está **ATIVADA** por padrão. Além de ter esta política habilitada, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima exigida. Se você habilitou a política e a versão do aplicativo Citrix Workspace é compatível,

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport é definido como **1** automaticamente no VDA. O Microsoft Teams lê a chave para carregar no modo VDI.

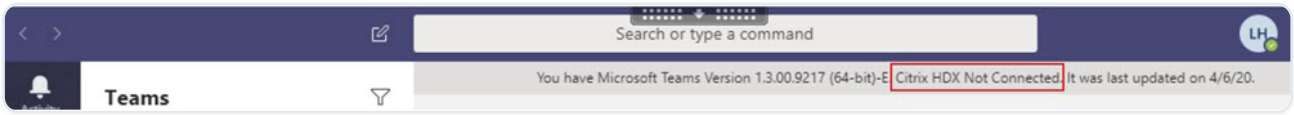
Nota:

Se você estiver usando VDAs versão 1906.2 ou posterior ou com versões de controlador mais antigas (por exemplo, versão 7.15) que não têm a política disponível no console de gerenciamento (Studio), seu VDA ainda poderá ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

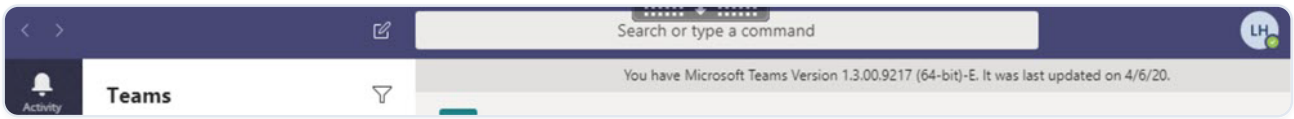
Se você clicar em **Sobre > Versão**, a legenda **Citrix HDX Optimized** será exibida:



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 do 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 compatível.



Importante: reconexões de sessão

- Pode ser necessário reiniciar o Microsoft Teams para obter uma sessão otimizada por HDX quando sua conectividade mudar. Por exemplo, se você estiver migrando de um endpoint não compatível (aplicativo Workspace para iOS, Android ou versões antigas de Windows/Linux/Mac) para um compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou vice-versa.

- Uma reinicialização do Microsoft Teams também é necessária se você instalou o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações VDI persistentes. Nesses casos, o Microsoft Teams pode ser atualizado automaticamente enquanto a sessão HDX está no estado desconectado. Assim, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado de forma otimizada.
- Ao migrar de uma sessão local para uma sessão HDX, você deve reiniciar o Microsoft Teams para otimizar com HDX. Esta ação é necessária em um cenário de Acesso Remoto a PC.

Requisitos de rede

O Microsoft Teams depende de servidores Media Processor no Microsoft 365 para reuniões ou chamadas multipartidárias. Além disso, o Microsoft Teams depende dos Microsoft 365 Transport Relays para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Assim, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Consulte Princípios de conectividade de rede do Microsoft 365 para obter diretrizes detalhadas sobre o planejamento de rede.

Recomendamos avaliar seu ambiente para identificar quaisquer riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem. Use a Ferramenta de Avaliação de Rede do Skype for Business para testar se sua rede está pronta para o Microsoft Teams. Para obter informações de suporte, consulte Suporte.

Resumo das principais recomendações de rede para tráfego de Protocolo de Tempo Real (RTP)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir do escritório da filial.
- Planeje e forneça largura de banda suficiente no escritório da filial.
- Verifique a conectividade e a qualidade da rede em cada escritório da filial.
- Se você precisar usar algum dos seguintes na filial, certifique-se de que o tráfego RTP/UDP (tratado por HdxRtcEngine.exe no aplicativo Citrix Workspace) não seja impedido.
    - Ignorar servidores proxy

- Interceptação SSL de rede
- Dispositivos de inspeção profunda de pacotes
- Hairpins de VPN (use tunelamento dividido, se possível)

Importante: Configuração de tunelamento dividido de VPN

O tráfego de HdxRtcEngine.exe deve ser desviado do túnel VPN e permitido usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira como isso é realizado varia dependendo do produto VPN e da plataforma da máquina utilizada, mas a maioria das soluções VPN permitirá alguma configuração simples de política para aplicar essa lógica. Para obter mais informações sobre a orientação de tunelamento dividido específica da plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o Protocolo de Transporte Seguro em Tempo Real (SRTP) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para este recurso, chaves simétricas (negociadas com DTLS) são usadas para criptografar mídia e mensagens de controle usando a cifra de criptografia AES.

As seguintes métricas são recomendadas para uma experiência de usuário positiva:

MÉTRICA	PONTO DE EXTREMIDADE PARA MICROSOFT 365
Latência (sentido único)	< 50 ms
Latência (RTT)	< 100 ms
Perda de Pacotes	<1% durante qualquer intervalo de 15s
Variação de atraso de chegada de pacotes (jitter)	<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.

Citrix Gateway

A presença de um Citrix Gateway local ou serviço Citrix Gateway como um proxy HDX não tem impacto na otimização do Microsoft Teams. Isso ocorre porque há apenas um canal virtual de comando e controle estabelecido entre o aplicativo Workspace e o VDA.

Todos os fluxos de áudio ou vídeo são descarregados para o cliente para processamento local. Como resultado, não há renderização no lado do servidor.

Dependendo da configuração em seu ambiente, o canal virtual de comando e controle flui através do Citrix Gateway usando uma das seguintes opções:

- TLS para TCP

- DTLS para EDT

Se você também estiver usando o Citrix Gateway para VPN, certifique-se de permitir que a máquina cliente alcance os servidores O365 Microsoft Teams diretamente. Você pode conseguir isso através de tunelamento dividido ou outros métodos.

Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração do 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 certificar-se de que `127.0.0.1:9002` seja ignorado.

  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 o estabelecimento de mídia de chamadas de conferência falharão.

- O local do servidor de conferência é selecionado com base na localização da área de trabalho virtual do primeiro participante (e não no cliente).

Estabelecimento de chamada e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão direta de rede Secure Real-time Transport Protocol (SRTP) sobre User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia retorna para TCP/TLS 443.

O mecanismo de mídia HDX oferece suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal Using Relays around NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Esse suporte significa que o endpoint deve ser capaz de realizar resoluções DNS.

Considere um cenário em que não há um caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está participando de uma chamada ou reunião multipartidária. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP de sub-rede do Microsoft 365 e quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver

bloqueado). Para obter mais informações, consulte o diagrama de arquitetura em Configuração de chamada e URLs e intervalos de endereços IP do Office 365 ID 11.

ID	CATEGORIA	ENDEREÇOS	PORTAS DE DESTINO
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (alternativa)

Esses intervalos incluem tanto os Transport Relays quanto os processadores de mídia, com um Azure Load Balancer como front-end. Os Transport Relays do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são endpoints ICE. Além disso, os Transport Relays do Microsoft Teams não encerram mídia, TLS ou realizam qualquer transcodificação. Eles podem fazer a ponte de TCP (se HdxRtcEngine.exe usar TCP) para UDP ao encaminhar tráfego para outros pares ou processadores de mídia.

O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com o Transport Relay do Microsoft Teams mais próximo na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e as portas UDP 3478–3481 (portas UDP diferentes por carga de trabalho, embora a multiplexação possa ocorrer) ou TCP/TLS 443 para alternativas. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado em vez do TCP, aconselhamos que você projete suas redes para acomodar o tráfego UDP no escritório remoto.

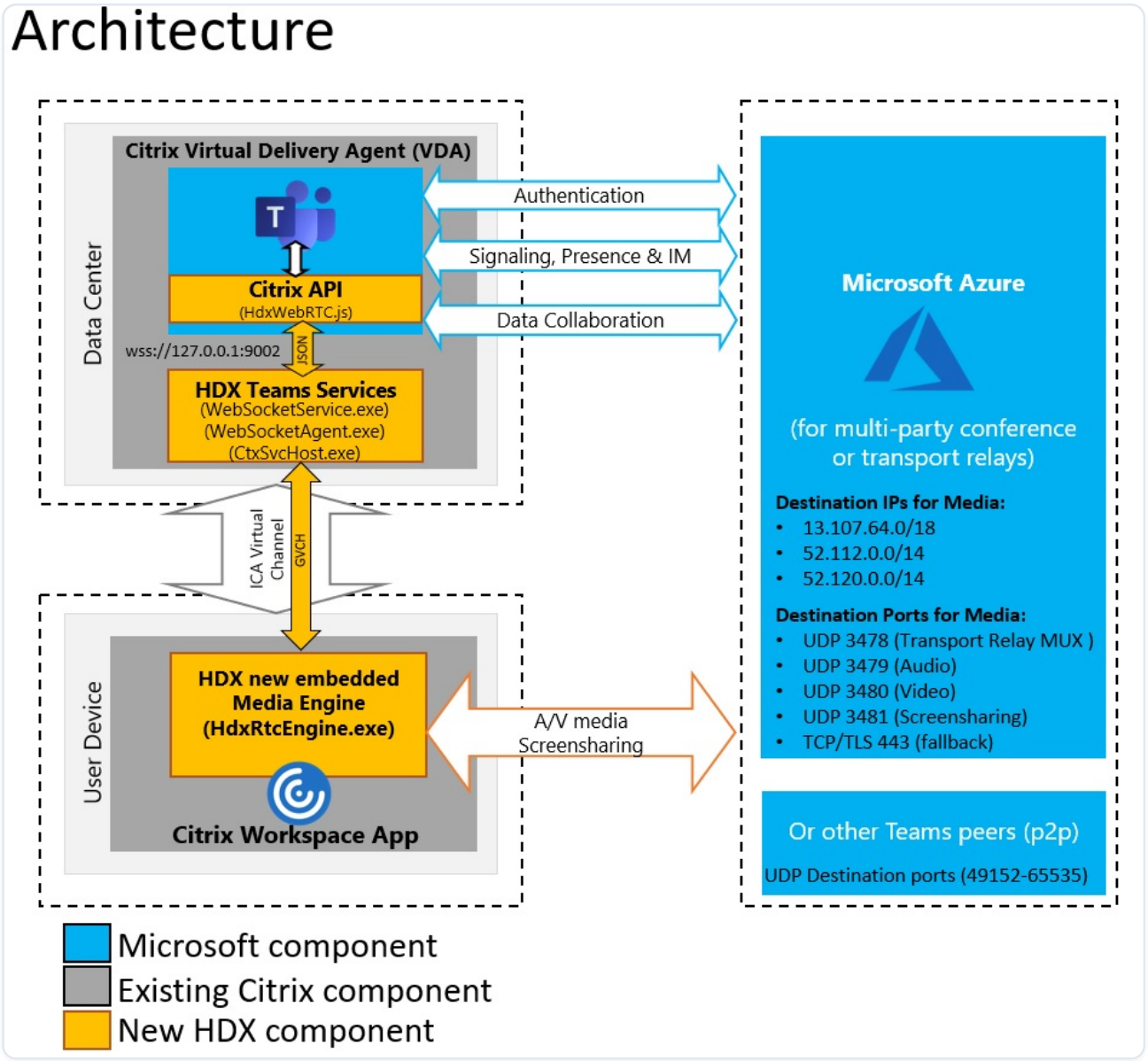
Se o Microsoft Teams for carregado no modo otimizado e HdxRtcEngine.exe estiver em execução no endpoint, falhas de ICE podem causar uma falha na configuração da chamada ou áudio/vídeo apenas unidirecional. Quando uma chamada não pode ser concluída ou os fluxos de mídia não são full duplex, verifique primeiro o **rastreamento do Wireshark** no endpoint. Para obter mais informações sobre o processo de coleta de candidatos ICE, consulte "Coleta de logs" na seção Suporte.

> **Nota:**
>
> Se os endpoints não tiverem acesso à internet, os usuários ainda poderão fazer uma chamada ponto a ponto se ambos estiverem na mesma LAN. As reuniões falham. Neste 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 (atravessamento de NAT e Firewall usando solicitações de ligação STUN) são concluídas. Em seguida, a mídia do Protocolo de Transporte em Tempo Real Seguro (SRTP) flui diretamente entre 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 o Microsoft Teams oferece suporte ao Phone System, usando Planos de Chamada do Microsoft 365 ou Roteamento Direto. Com o Roteamento Direto, você conecta seu próprio controlador de borda de sessão compatível diretamente ao Microsoft Phone System sem nenhum software local adicional. Filas de chamadas, transferência, encaminhamento, espera, mudo e retomada de uma chamada são suportados.

DTMF

O recurso de multifrequência de tom duplo (DTMF) é suportado com estas versões do aplicativo Citrix Workspace (e posteriores):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para Chrome OS versão 2111.1

Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado em Planos de Chamada da Microsoft, Operator Connect e Roteamento Direto, ele permite que você faça o seguinte:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace que é executado no endpoint, em vez do cliente Microsoft Teams que é executado no VDA.

A lei de Ray Baum exige que a localização despachável do chamador do 911 seja transmitida ao Ponto de Atendimento de Segurança Pública (PSAP) apropriado. A otimização do Microsoft Teams com HDX está em conformidade com a lei de Ray Baum quando usada com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Linux versão 2112 e posterior
- Aplicativo Citrix Workspace para Mac versão 2112 e posterior
- Aplicativo Citrix Workspace para Chrome OS versão 2112 e posterior

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de rede ou de localização de emergência:

- Configurações de rede
- Serviço de Informações de Localização (LIS)

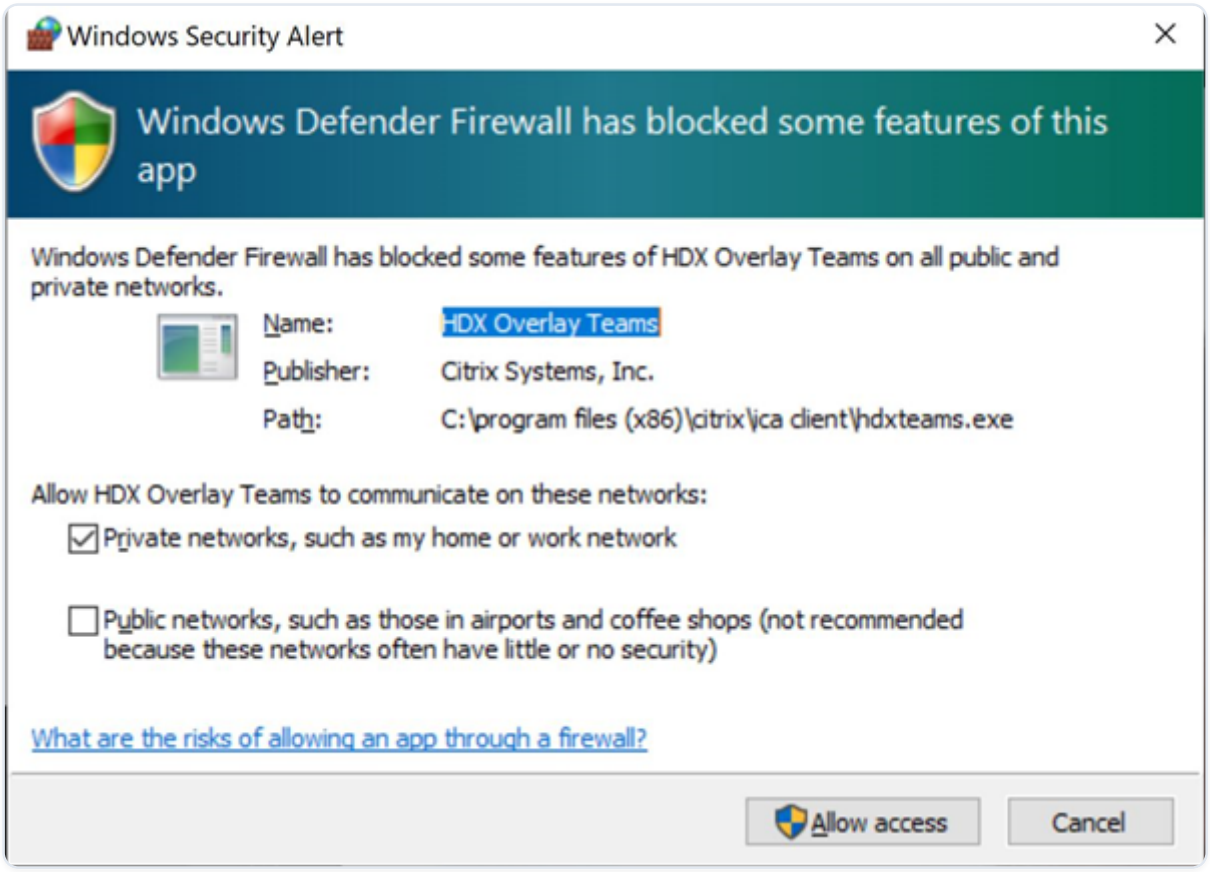
Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de localização despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

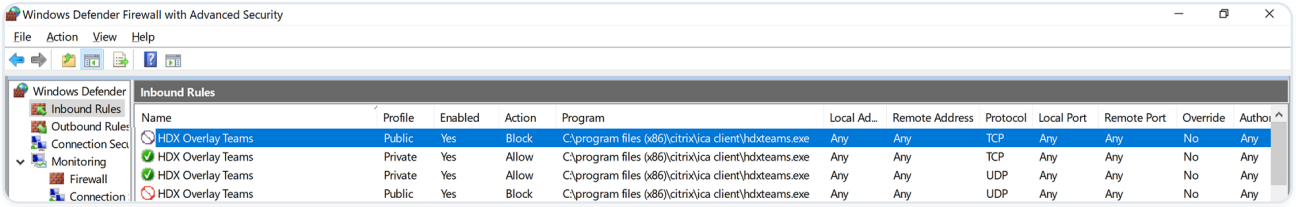
- ID do Chassi / ID da Porta usando o Protocolo de Descoberta da Camada de Link (LLDP) para conexões Ethernet/Switch. Ethernet/Switch (LLDP) é suportado em:
  - Versões do Windows 8.1 e 10
  - macOS, que requer software de habilitação LLDP
  - Linux, que requer que a biblioteca LLDP seja incluída na 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)
  - Suportado em 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 libgps-dev 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.



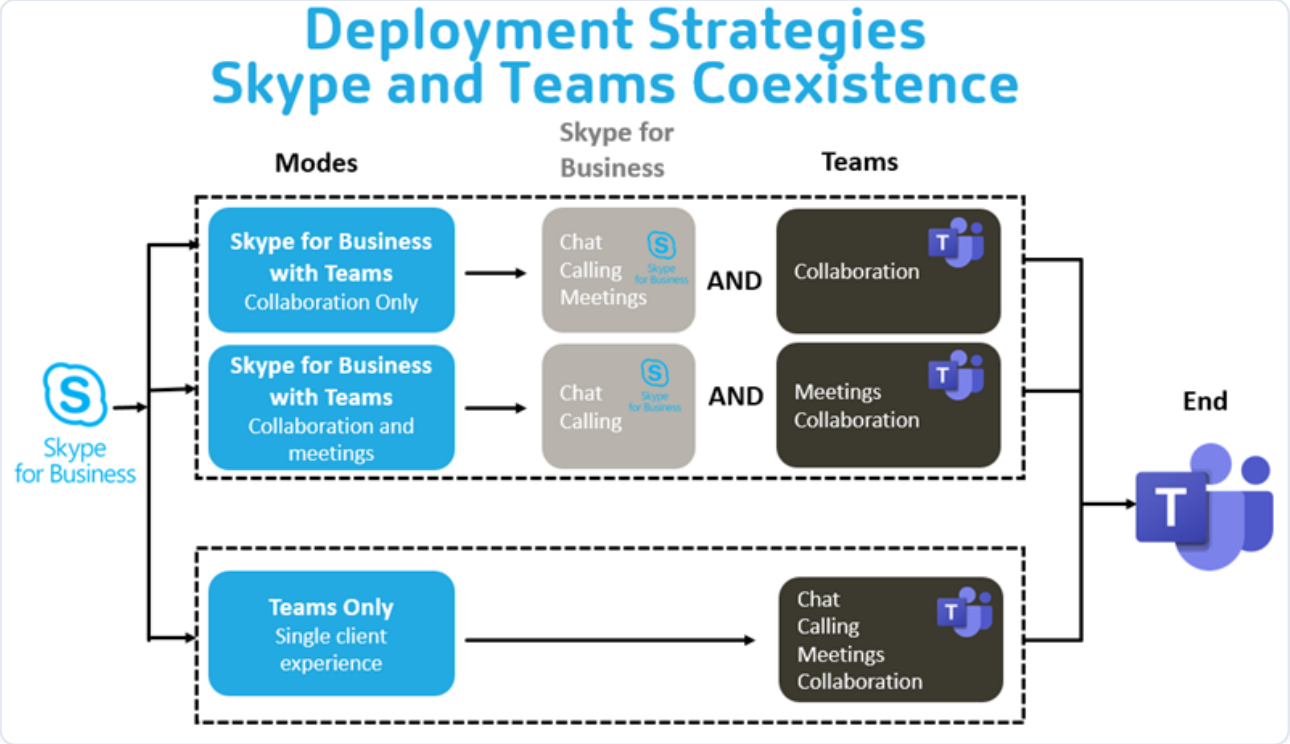
Coexistência do Microsoft Teams e do Skype for Business

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 honram a configuração definida em seu ambiente. Os exemplos incluem modos de ilha e Skype for Business com colaboração do Microsoft Teams. Além disso, Skype for Business com colaboração e reuniões do Microsoft Teams.

O acesso a periféricos pode ser concedido a apenas um aplicativo por vez. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem

durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



Citrix SD-WAN™: conectividade de rede otimizada para o Microsoft Teams

A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio e vídeo do Microsoft Teams de usuários do Citrix Workspace app em filiais para um data center antes de ir para a internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço web do Microsoft 365 baseado em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

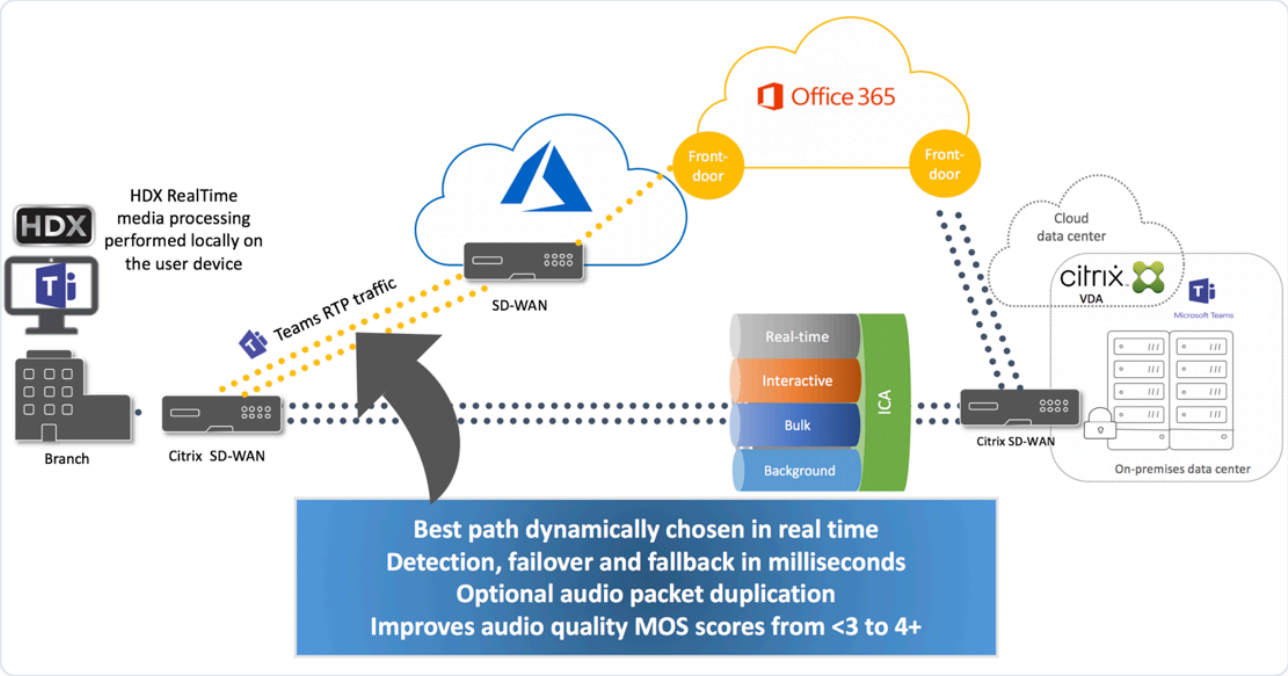
As conexões de internet banda larga empresarial em muitas áreas sofrem com perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio e vídeo do Microsoft Teams quando a integridade da rede é variável ou degradada.

- Se você usa o Microsoft Azure, um appliance virtual Citrix SD-WAN (VPX) implantado na VNET do Azure oferece otimizações avançadas de conectividade. Essas otimizações incluem failover de link contínuo e corrida de pacotes de áudio.

- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud™ Direct. Este serviço oferece entrega confiável e segura para todo o tráfego destinado à internet.

Se a qualidade da conexão de internet da filial não for uma preocupação, pode ser suficiente minimizar a latência. Direcione o tráfego do Microsoft Teams diretamente do appliance de filial do Citrix SD-WAN para o front door mais próximo do Microsoft 365 para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo em várias janelas

Você pode usar várias janelas de reunião ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Janelas Pop-Out do Microsoft Teams para Bate-papos e Reuniões no site do Microsoft 365.

> **Nota:**
>
> Este recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203 e VDA 2112.

Visualização de galeria e oradores ativos no Microsoft Teams

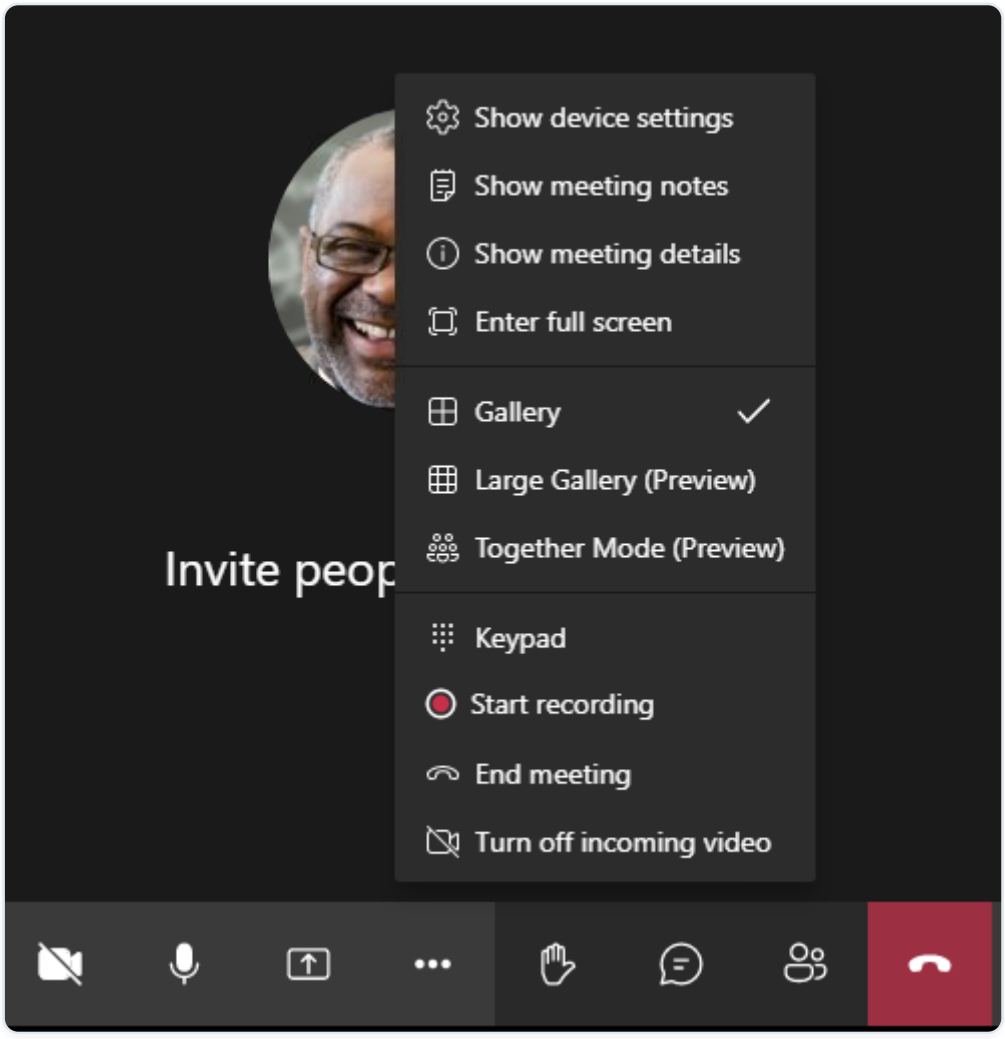
O Microsoft Teams oferece suporte aos layouts **Galeria**, **Galeria grande** e **Modo Juntos**.

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 vídeo, apenas os quatro oradores mais ativos aparecem na tela.

O Microsoft Teams também oferece a visualização de galeria grande com uma grade de até 7x7. Como resultado, o servidor de conferência do Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Esse feed único, estilo matriz, também pode incluir o vídeo de auto-visualização dos usuários.

Por fim, o Microsoft Teams oferece suporte ao **Modo Juntos**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para posicionar digitalmente os participantes em um plano de fundo compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada de conferência selecionando os layouts **Galeria**, **Galeria grande** ou **Modo Juntos** no menu de reticências.



Suporte para restrições de proporção de vídeo (CWA para Windows 2102, CWA para Linux 2106, CWA para MAC 2106 e posterior):

- A opção **Preencher para enquadrar** está disponível na Visualização de Galeria/Galeria Grande. Esta opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts de Galeria e Galeria Grande:

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
Layout / Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro oradores mais ativos aparecem na tela e outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.
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 único fluxo de vídeo de qualidade. Você pode definir o valor da resolução de codificação no cliente. Para obter mais informações, consulte Estimador de desempenho do codificador e Otimização para Microsoft Teams. A qualidade é definida como resolução e	Um único fluxo de vídeo de qualidade. Você pode definir o valor da resolução de codificação no cliente. Para obter mais informações, consulte Estimador de desempenho do codificador e Otimização para Microsoft Teams.

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
	quadros por segundo. Atualmente, o vídeo simulcast não é compatível.	
Decodificação no endpoint	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no endpoint pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo para áudio e vídeo. Essa configuração reduz o consumo de CPU no endpoint.
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é de 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo pode ser maior.	720p para o layout composto ou mixagem. Não há necessidade de um fluxo de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente reduz a resolução ou a taxa de bits de upload.
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

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
		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 ou Mac, os usuários podem compartilhar suas telas e câmera de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera será pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O colega deve então retomar manualmente o compartilhamento da câmera.

Observação para 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 Citrix Workspace app. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Qualquer aplicativo local que se sobreponha ao Desktop Viewer não é capturado.

Nota

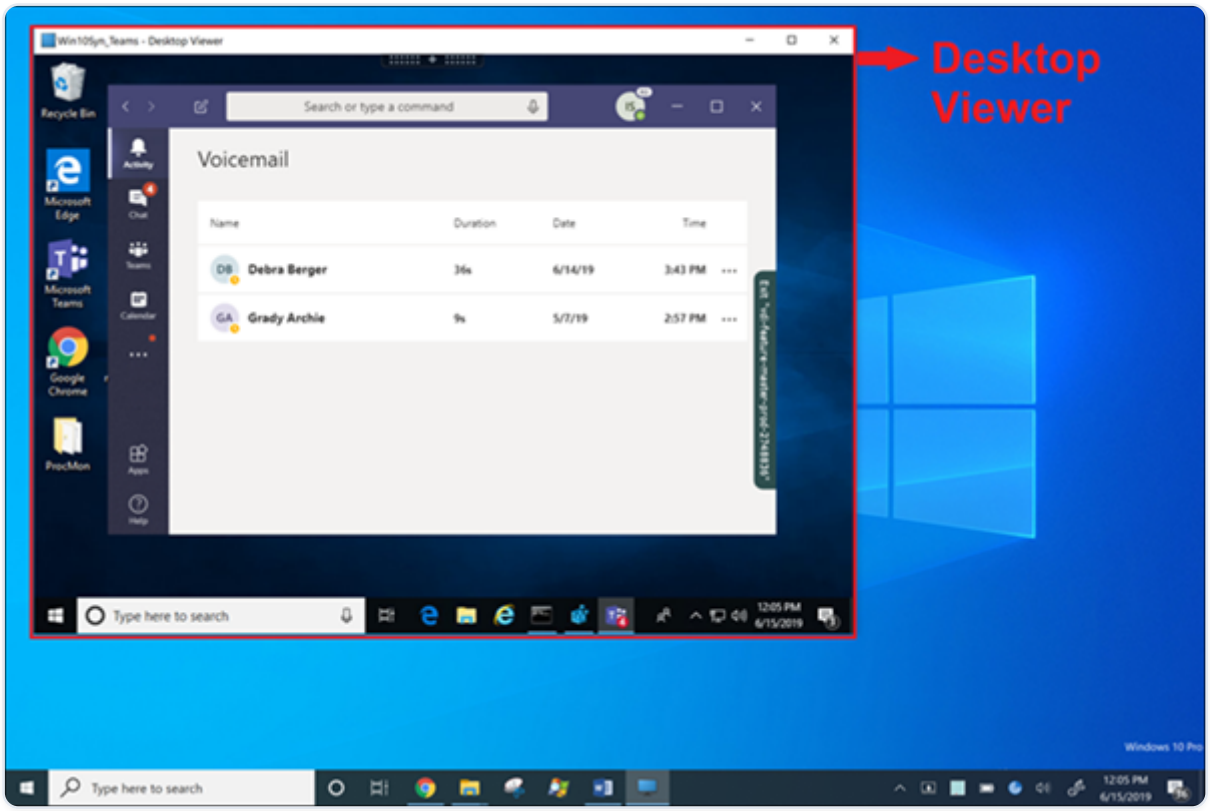
> Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

Multimonitor

Se o Desktop Viewer (CDViewer.exe) estiver em modo de tela cheia e abrangendo configurações de vários monitores, o aplicativo Citrix Workspace 2106 ou posterior (Windows/Linux/Mac) permite que o seletor de tela escolha o monitor a ser compartilhado.

Limitação conhecida:

- Se o Desktop Viewer estiver desabilitado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desabilitado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela em vários monitores.
- Em versões do aplicativo Workspace anteriores à 2106, apenas o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor principal para que o outro participante da chamada possa vê-lo.
- O compartilhamento de tela em vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout de monitor virtual (partição lógica de um único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.
- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento é possível apenas se o aplicativo local estiver sobreposto ao Desktop Viewer. Esse comportamento foi removido nas versões 2009.6 ou superiores e 1912 CU5 ou superiores.



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 usando o HDX 3D Pro.

A partir do aplicativo Citrix Workspace para Windows 2109, Mac 2203 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Para compartilhar um aplicativo específico:

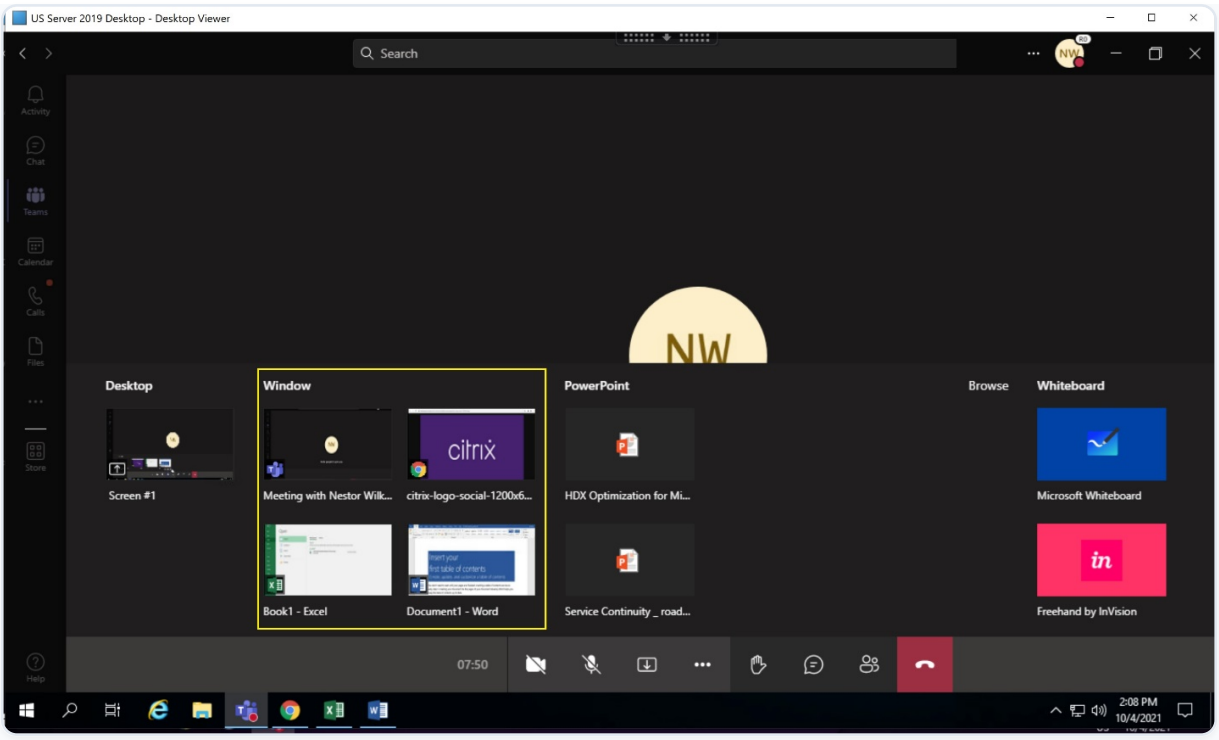
1. navegar para o aplicativo Microsoft Teams dentro da sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo selecionado e os participantes da chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desabilitar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`: Nome: `UseWsProvider` Tipo: `DWORD` Valor: 0

Nota:

- Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
- O compartilhamento de tela depende da captura da janela no lado do VDA. O conteúdo é então retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para os pares ou para o servidor de conferência.



Limitações conhecidas com o compartilhamento de tela de aplicativos específicos:

- O ponteiro do mouse não fica visível ao compartilhar a tela de um aplicativo.
- Se você minimizar um aplicativo enquanto o estiver compartilhando, apenas o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até que você maximize o aplicativo.

Compatibilidade com a proteção de aplicativos O compartilhamento de tela de um aplicativo específico é compatível com o recurso de proteção de aplicativos no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico se tiver iniciado o aplicativo ou a área de trabalho de um grupo de entrega que tenha a proteção de aplicativos ativada.

Ao clicar em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Desktop**. Você só pode selecionar a opção **Janela** para compartilhar qualquer aplicativo aberto.

> **Nota:**
>
> Ao iniciar aplicativos ou áreas de trabalho de um grupo de entrega com proteção de aplicativo ativada, você não consegue ver o vídeo ou o compartilhamento de tela de entrada se estiver usando o aplicativo Workspace para Windows 2202 ou anterior. Essa limitação não está presente no aplicativo Workspace para Windows 2203 LTSR e posterior.

Conceder e solicitar controle no Microsoft Teams

Este recurso é compatível com as seguintes versões do aplicativo Citrix Workspace (não há dependência da versão do VDA ou do sistema operacional, sessão única ou multissessão):

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 e posterior

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de ter o controle, você pode fazer seleções, edições ou outras atividades de teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela estiver sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar sua solicitação.

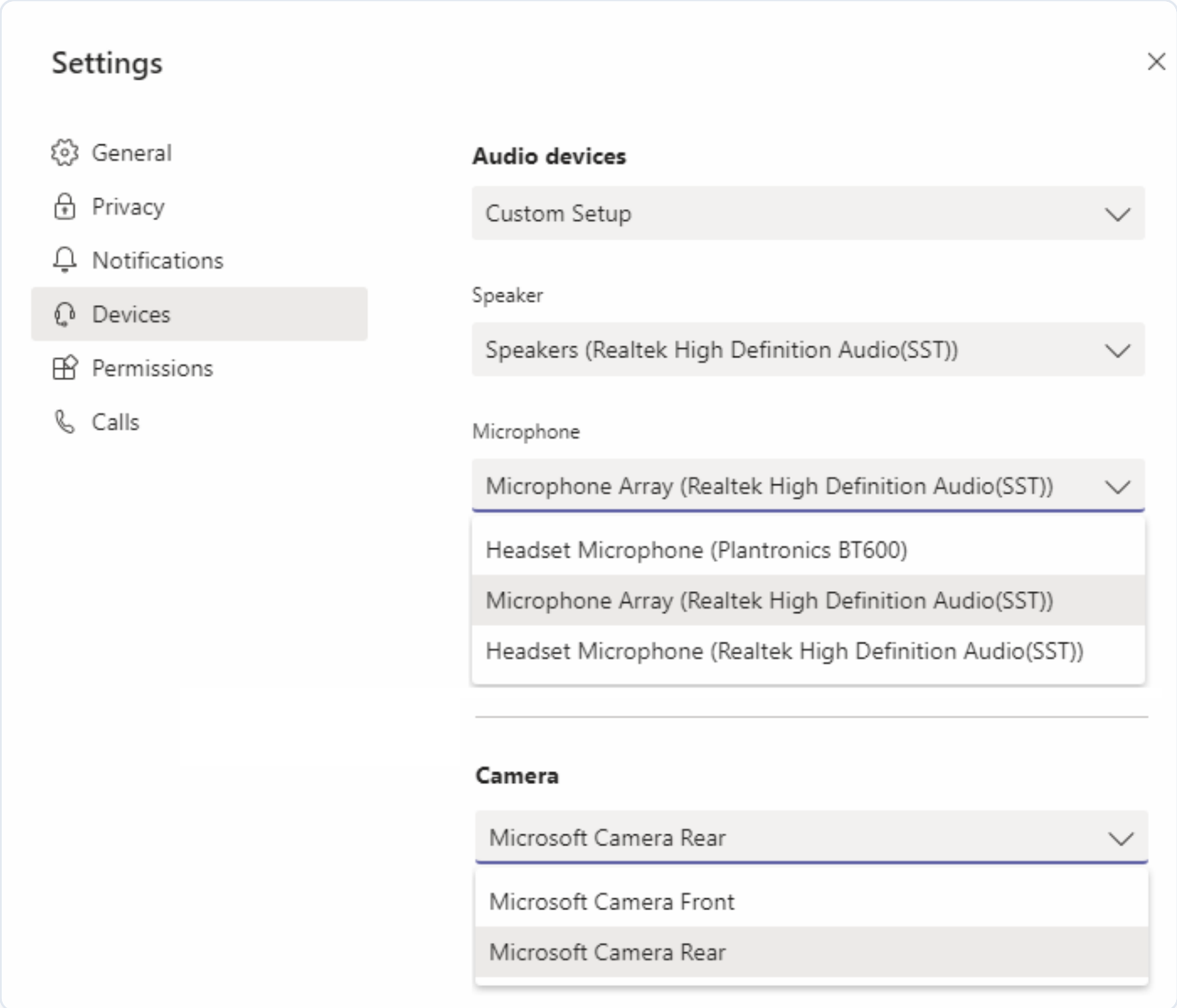
Enquanto você tiver o controle, poderá fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar o teclado e o mouse. Quando terminar, clique em **Solicitar controle**.

> **Limitações:**

- Conceder e Solicitar controle não estão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como Compartilhamento de aplicativo). A área de trabalho ou o monitor completo deve ser compartilhado.
- O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização para Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fones de ouvido, microfones, câmeras, alto-falantes e assim por diante). Então, os periféricos são listados corretamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele depende do mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão do mesmo endpoint.

Recomendações:

- Fones de ouvido certificados para Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde microfone e alto-falantes estão em dispositivos separados, pode haver um eco. Um exemplo é uma webcam com microfone integrado e um monitor com alto-falantes. Ao usar alto-falantes externos, posicione-os o mais longe possível do microfone. Além disso, posicione-os longe de qualquer superfície que possa refratar o som para o microfone.
- Câmeras certificadas para Microsoft Teams, embora periféricos certificados para Skype for Business sejam compatíveis com o Microsoft Teams.
- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento da CPU com webcams que realizam codificação H.264 integrada - UVC 1.1 e 1.5.

> **Nota:**
>
> O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio de 24 bits ou com frequências acima de 96 kHz.
>
> HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou anterior) suporta apenas estes formatos específicos de dispositivo de áudio (canais, profundidade de bits e taxa de amostragem):
>
> - Dispositivos de Reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
> - Dispositivos de Gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz
>
> Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.

Os logs do **Webrpc** em **HdxTeams.exe** mostram este tipo de informação:

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

Como solução alternativa, desative o dispositivo específico ou:

1. Abra o **Painel de Controle de Som** (mmsys.cpl).
2. Selecione o dispositivo de reprodução ou gravação.
3. Vá para **Propriedades > Avançado** e altere as configurações para um modo compatível.

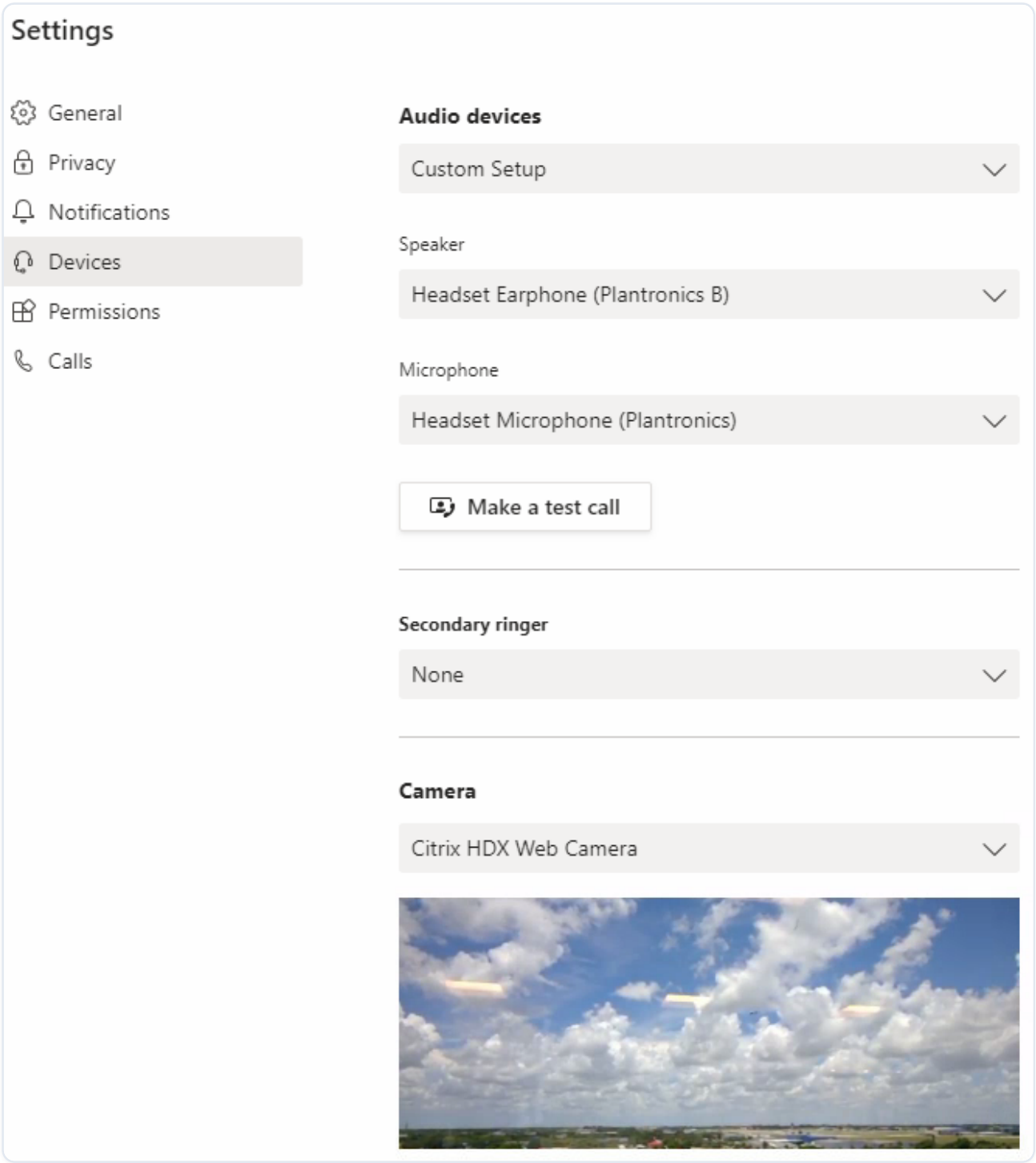
Modo de fallback

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Not Connected" em Teams/Sobre/Versão), o VDA retorna às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento de webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão do aplicativo Workspace/SO de plataforma que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam. No modo de fallback, os periféricos são mapeados para o VDA. Os periféricos aparecem para o aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no VDA. Para obter informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados por meio do registro.

Este recurso requer a versão 1.3.0.13565 ou posterior do Microsoft Teams.

Para determinar se você está no modo otimizado ou não otimizado ao visualizar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX legadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX**, conforme mostrado na imagem a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) em comparação com o modo otimizado.



Quando tecnologias HDX legadas são usadas, o Microsoft Teams não descarrega o processamento de áudio, vídeo e compartilhamento de tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do endpoint. Em vez disso, as tecnologias HDX usam renderização do lado do servidor. Espere alto consumo de CPU no VDA ao ligar o vídeo. O desempenho de áudio em tempo real pode não ser ideal.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- As configurações de QoS no Centro de Administração para Microsoft Teams não se aplicam a usuários VDI.
- Os usuários não podem tirar capturas de tela do conteúdo do Teams se usarem uma ferramenta de recorte no VDA. Somente se usado no lado do cliente o conteúdo pode ser capturado.

Limitação no VDA:

- Quando você configura a configuração de DPI Alto do aplicativo Citrix Workspace para **Sim**, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente — não no VDA.

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 em vez disso).
- A função de zoom in e zoom out no Microsoft Teams não é suportada.
- O Roteamento Baseado em Localização e o Desvio de Mídia não são suportados.
- A integridade da chamada não está disponível.

- As salas de apoio são compatíveis com participantes VDI. O Microsoft Teams não oferece suporte a salas de apoio se o organizador for um usuário VDI.
- 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 está disponível.
- **Campainha secundária** (**Teams** > **Configurações** > **Dispositivos**) não é compatível.
- As opções para desfocar ou personalizar o plano de fundo não são suportadas.

Próximo EOL do Microsoft Teams de Janela Única

Em January 31, 2024, a Microsoft descontinuará o suporte do Microsoft Teams para a interface de usuário de janela única ao usar a otimização do Microsoft Teams VDI e suportará apenas a experiência de múltiplas janelas. A Microsoft notificou essa descontinuação em 9/8/2023 no Centro de Administração do M365 (ID da Postagem: MC674419). Detalhes públicos sobre o recurso de Múltiplas Janelas podem ser encontrados no artigo da Comunidade Técnica: New Meeting and Calling Experience in Microsoft Teams.

Você deve atualizar seu VDA e o aplicativo Citrix Workspace para as versões suportadas para continuar usando o Microsoft Teams no modo otimizado para vídeo e compartilhamento de tela. Se você não atualizar sua infraestrutura e endpoints para suportar múltiplas janelas, você poderá apenas estabelecer chamadas de áudio. Você não poderá usar a funcionalidade otimizada de vídeo e compartilhamento de tela.

A tabela a seguir ilustra as versões mínima, LTSR e recomendada do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams em Citrix VDI:

COMPONENTE	VERSÃO MÍNIMA	VERSÃO LTSR SUPORTADA	VERSÃO RECOMENDADA
Microsoft Teams	1.5.00.11865	Não aplicável	Mais recente
VDA	1912 CU6 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+

COMPONENTE	VERSÃO MÍNIMA	VERSÃO LTSR SUPORTADA	VERSÃO RECOMENDADA
Aplicativo Citrix Workspace para Windows	2205 CR	2203 CU2+	2309 CR+
Aplicativo Citrix Workspace para Mac	2209 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para Linux	2209 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para ChromeOS ou HTML5	2303 CR	Não aplicável	2309 CR+

Anúncio de descontinuação do formato SDP (Plano B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP atual (Plano B) do WebRTC em futuras versões. Você deve usar o Plano Unificado no WebRTC para oferecer suporte às funcionalidades otimizadas do Microsoft Teams.

Produtos afetados

Em uma das futuras versões do Citrix Workspace Application, chamadas entre endpoints com a próxima versão do aplicativo Citrix Workspace e endpoints com o aplicativo Citrix Workspace 2108 ou versões mais antigas não serão suportadas. Essa incompatibilidade de chamada inclui clientes do aplicativo Citrix Workspace 1912 LTSR (CWA). Os seguintes clientes CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

Substituição para o Plano B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior a 2109, você deve atualizar para uma versão suportada (preferencialmente a versão CR mais recente). Caso contrário, quaisquer chamadas com uma versão futura ou endpoints mais recentes falharão ao

conectar. Chamadas entre versões futuras e seus parceiros de comunicação federados também podem falhar ao serem concluídas se o parceiro federado não tiver atualizado seu Citrix Workspace.

A versão 2108 do aplicativo Citrix Workspace encerrou sua data de suporte em março de 2023 e deve ser atualizada para uma versão mais recente. Para obter mais informações, consulte Workspace App para detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plano B, consulte a documentação WebRTC.

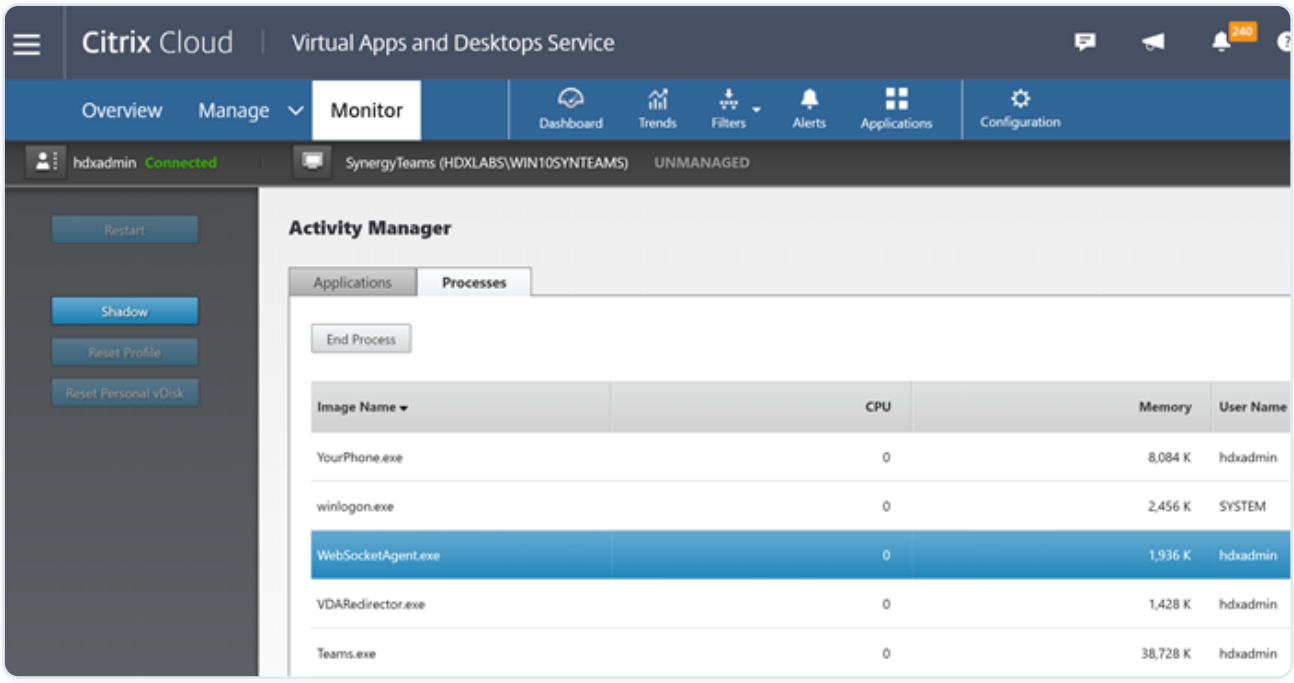
Informações adicionais

- 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 **Gerenciador de Atividades** no Director para ver o aplicativo.



Com a versão mínima 1912 do VDA, você pode monitorar chamadas ativas do Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`.

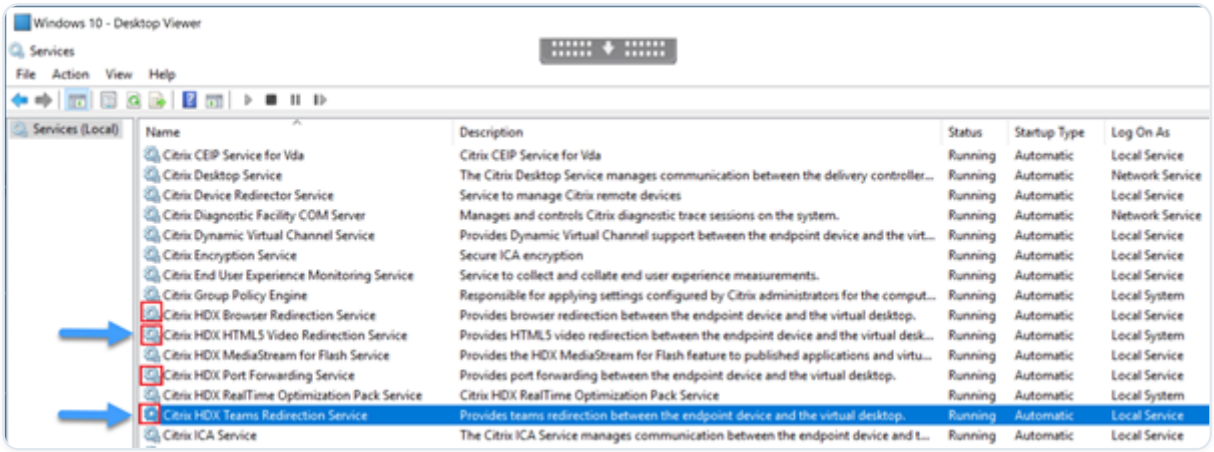
Para obter mais informações, consulte *Monitoramento* no artigo da Central de Conhecimento CTX253754.

Solução de problemas

Esta seção fornece dicas de solução de problemas para questões que você pode encontrar ao usar a otimização para Microsoft Teams. Para obter mais informações, consulte CTX253754.

No Virtual Delivery Agent

Existem quatro serviços instalados por BCR_x64.msi. Apenas dois são responsáveis pelo redirecionamento do Microsoft Teams no VDA.



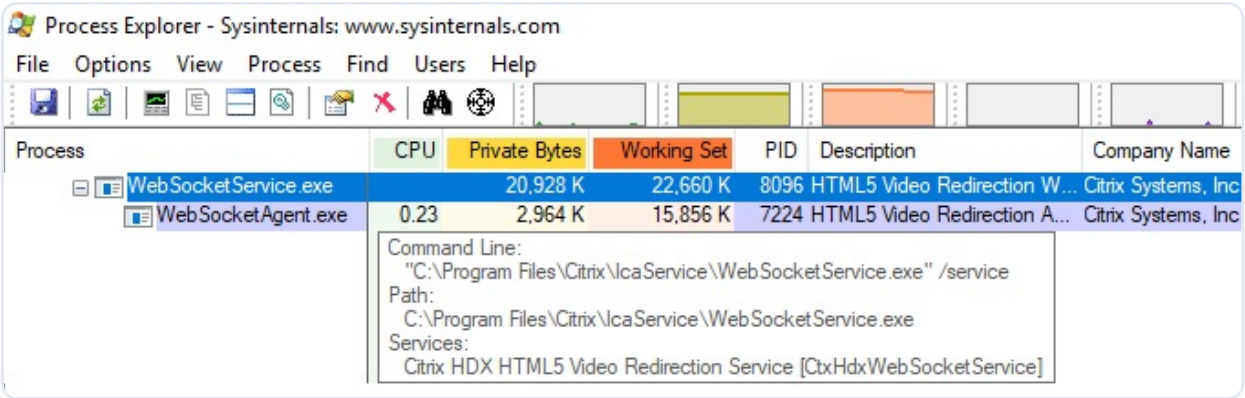
- O **Serviço de Redirecionamento do Citrix HDX Teams** estabelece o canal virtual usado no Microsoft Teams. O serviço depende de CtxSvcHost.exe.
- O **Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX** é executado como WebSocketService.exe, escutando em 127.0.0.1:9002 TCP. WebSocketService.exe 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 de Redirecionamento de Vídeo HTML5 do Citrix HDX possa estar em execução no console `services.msc`, o socket TCP `127.0.0.1:9002` do localhost nunca está no modo de escuta, como visto no netstat. Tentar reiniciar o serviço faz com que ele trave ("Parando..."). Certifique-se de aplicar as exclusões adequadas para o processo `WebSocketService.exe`.



  ii. **Mapeamento de sessão do usuário.** Quando o aplicativo Microsoft Teams é iniciado, WebSocketService.exe inicia o processo WebSocketAgent.exe na sessão do usuário no VDA. 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` em 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:

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.

Locais e descrições dos serviços

SERVIÇO	CAMINHO PARA O EXECUTÁVEL NO SO WINDOWS SERVER	FAZER LOGON COMO	DESCRIÇÃO
Serviço de Redirecionamento de Vídeo HTML5 da Citrix	"C:\Arquivos de Programas (x86)\Citrix\System32\WebSocketService.exe" /service	Conta do Sistema Local	Fornece múltiplos serviços HDX Multimedia com a estrutura inicial necessária para realizar o redirecionamento de mídia entre o desktop virtual e o dispositivo de endpoint.

SERVIÇO	CAMINHO PARA O EXECUTÁVEL NO SO WINDOWS SERVER	FAZER LOGON COMO	DESCRIÇÃO
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 Equipes 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 que você instalou no mínimo a Workspace App versão 1905 para Windows. Você vê HdxTeams.exe ou HdxRtcEngine.exe e os binários 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 otimização para Microsoft Teams. Este suporte conjunto é o resultado de uma estreita colaboração entre as duas empresas. Se você tiver contratos de suporte válidos e encontrar um problema com esta solução, abra um tíquete de suporte com o fornecedor cujo código você suspeita estar causando o problema. Ou seja, Microsoft para Teams ou Citrix para os componentes de otimização. A Citrix ou a Microsoft recebe o tíquete, avalia o problema e o escala conforme apropriado. Não há necessidade de você entrar em contato com a equipe de suporte de cada empresa.

Quando tiver um problema, recomendamos que clique em **Ajuda > Relatar um Problema** na interface do usuário do Teams. Os logs do lado do VDA são compartilhados automaticamente entre a Citrix e a Microsoft para resolver problemas técnicos mais rapidamente.

Coletando logs

Os logs do mecanismo de mídia HDX podem ser encontrados na máquina do usuário (não no VDA). Em caso de problemas, certifique-se de anexar os logs ao seu caso de suporte.

Logs do Windows:

Você pode localizar os logs do Windows em %TEMP% dentro da pasta **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Procure por um arquivo .txt chamado webrpc_Dia_Mês_carimbo_de_data_hora_Ano.txt. Se você estiver usando versões mais

recentes do aplicativo Citrix Workspace, por exemplo, Citrix Workspace app 2009.5 ou posterior, armazene os logs em AppData\Local\Temp\HdxRtcEngine.

Cada sessão cria uma pasta separada para os logs.

Logs do Mac:

1. Log VDWEBRTC - registra a execução do canal virtual.

   Localização: `/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. Log HdxRtcEngine - registra a execução dos processos no HdxRtcEngine.

   Localização: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   O log HdxRtcEngine é habilitado por padrão.

3. Logs Webrpc - são os logs mais importantes que registram a execução do wrap-up da biblioteca webrtc.

   Localização: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Logs do Linux:

Você pode localizar os logs do Linux nas pastas `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`. Log 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. Veja 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
```

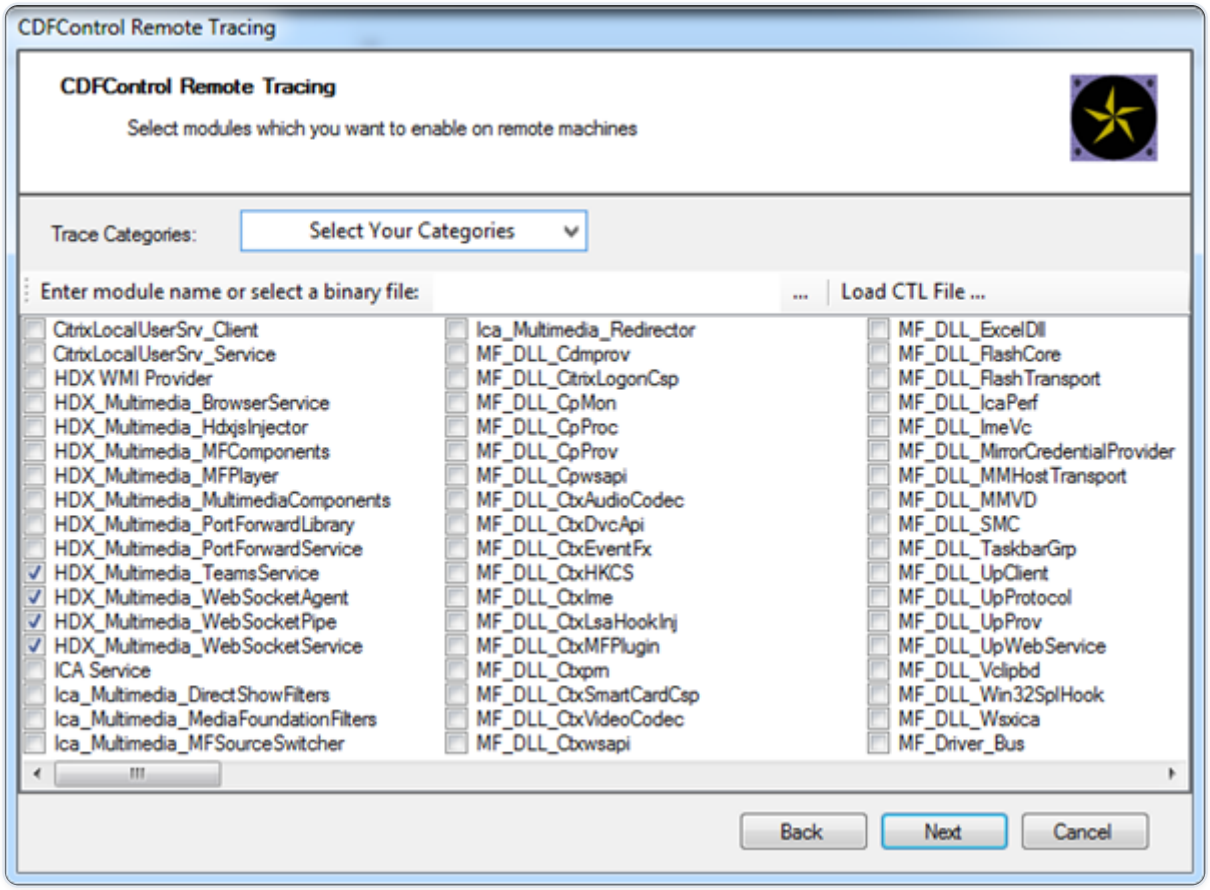
Se houver vários candidatos ICE, a ordem de preferência é:

1. Máquina
2. reflexivo de par
3. reflexivo de servidor
4. relay de transporte

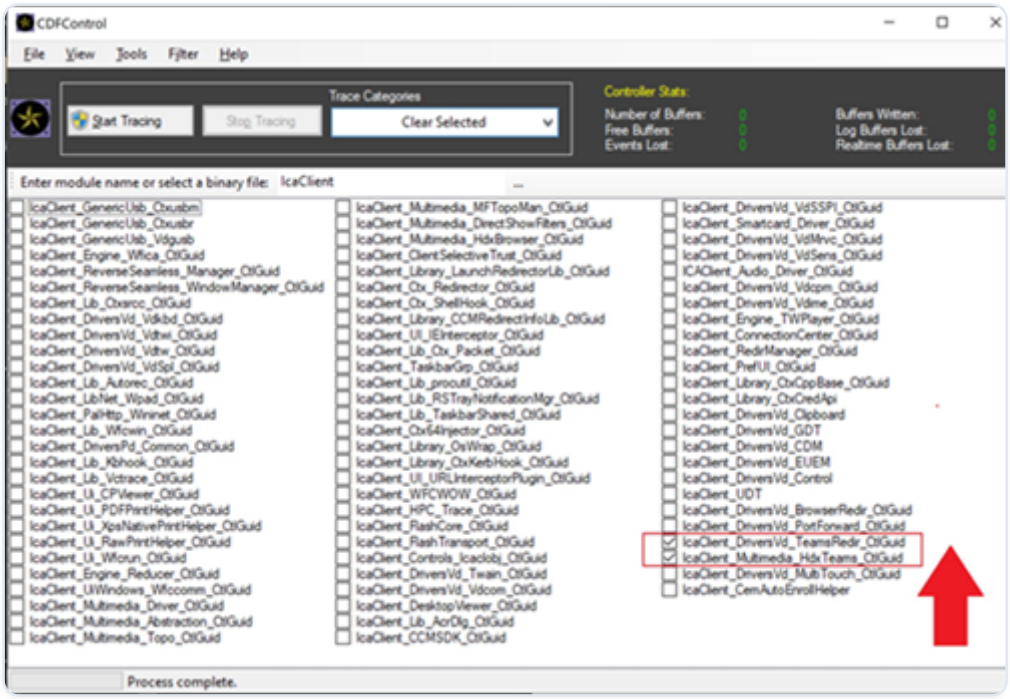
Se você encontrar um problema e puder reproduzi-lo consistentemente, recomendamos que clique em **Ajuda > Relatar um problema** no Teams. Os logs são compartilhados entre a Citrix e a Microsoft para resolver problemas técnicos, caso você tenha aberto um caso com a Microsoft. A captura de rastreamentos CDF antes de entrar em contato com o Suporte Citrix também é benéfica. Para obter mais informações, consulte o artigo da Central de Conhecimento CDFcontrol.

Para recomendações sobre a coleta de rastreamentos CDF, consulte o artigo da Central de Conhecimento Recomendações para Coletar os Rastros CDF.

Rastreamentos CDF do lado do VDA - Habilite os seguintes provedores de rastreamento CDF:



Rastreamentos CDF do lado do aplicativo Workspace - Habilite os seguintes provedores de rastreamento CDF:



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requer o aplicativo Citrix Workspace 2012 ou posterior)

Redirecionamento de Mídia do Windows

O redirecionamento de Mídia do Windows controla e otimiza a forma como os servidores entregam áudio e vídeo 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. Esse método é transparente para os usuários. Você pode usar o Citrix Scout para realizar um rastreamento do Citrix Diagnosis Facility (CDF) de HostMMTransport.dll para determinar o método usado. Para obter mais informações, consulte Citrix Scout.

O redirecionamento de Mídia do Windows intercepta o pipeline de mídia no servidor host, captura os dados de mídia em seu formato compactado nativo e redireciona o conteúdo para o dispositivo cliente. O dispositivo cliente então recria o pipeline de mídia para descompactar e renderizar os dados de mídia recebidos do servidor host. O redirecionamento de Mídia do Windows funciona bem em dispositivos cliente que executam um sistema operacional Windows. Esses dispositivos possuem a estrutura multimídia necessária para reconstruir o pipeline de mídia como existia no

servidor host. Clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento de Mídia do Windows** controla esse recurso e é **Permitida** por padrão. Geralmente, essa configuração aumenta a qualidade de áudio e vídeo renderizada do servidor para um nível comparável ao conteúdo reproduzido localmente em um dispositivo cliente. Em casos raros, a reprodução de mídia usando o redirecionamento de Mídia do Windows parece pior do que a mídia renderizada usando a compactação ICA® básica e áudio regular. Você pode desabilitar esse recurso adicionando a configuração **Redirecionamento de Mídia do Windows** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações de política, consulte Configurações de política de multimídia.

Limitação:

Ao usar o Windows Media Player e as Extensões de Áudio e Vídeo Remoto (RAVE) ativadas dentro de uma sessão, uma tela preta pode aparecer. Essa tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Em Reprodução no topo**.

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/2203-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/2203-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/2203-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™ fornece **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 e 64 bits (versão mínima 1607)
- Windows 8.1, edições de 32 e 64 bits (incluindo a edição Embedded)
- Windows 7, edições de 32 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 do host para o cliente

O redirecionamento do host para o cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix®, sejam abertas usando o aplicativo correspondente no dispositivo de endpoint do usuário. Alguns casos de uso comuns para o redirecionamento do host para o cliente incluem:

- Redirecionamento de sites em casos em que o servidor Citrix não tem acesso à Internet ou à rede para a origem.
- Redirecionamento de sites quando a execução de um navegador da web dentro da sessão Citrix não é desejada por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos em casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento do host para o cliente não se destina a URLs que você acessa em uma página da web ou digita na barra de endereços do navegador da web em execução na sessão Citrix. Para redirecionamento de URLs em navegadores da web, consulte Redirecionamento de URL bidirecional ou Redirecionamento de conteúdo do navegador.

Requisitos do sistema

- VDA de SO multissessão
- Clientes compatíveis:
  - Citrix Workspace™ app para Windows
  - Aplicativo Citrix Workspace para Mac
  - Aplicativo Citrix Workspace para Linux
  - Aplicativo Citrix Workspace para HTML5
  - Aplicativo Citrix Workspace para Chrome

O dispositivo cliente deve ter um aplicativo instalado e configurado para lidar com o redirecionamento dos tipos de URL.

Configuração

Use a política Citrix de Redirecionamento do host para o cliente para habilitar essa 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** em combinação com as chaves **DisableServerFTA** e **NoRedirectClasses**.

Configuração do navegador padrão do VDA do servidor

A habilitação do redirecionamento do host para o cliente, conforme referenciado nesta seção, substitui qualquer configuração de navegador padrão anterior no VDA do servidor. Se uma URL da web não for redirecionada, o Citrix Launcher passará a URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente. Para obter mais informações, consulte Configuração do navegador padrão do VDA do servidor na lista de recursos gerenciados por meio do registro.

Redirecionamento de conteúdo bidirecional

O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS em navegadores da web, ou incorporadas em aplicativos, sejam encaminhadas entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Uma URL inserida em um navegador em execução na sessão Citrix pode ser aberta usando o navegador padrão do cliente. Por outro lado, uma URL inserida em um navegador em execução no cliente pode ser aberta em uma sessão Citrix, seja com um aplicativo ou desktop publicado. Alguns casos de uso comuns para o redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da web em casos em que o navegador inicial não tem acesso à rede para a origem.

- Redirecionamento de URLs da web por motivos de compatibilidade do navegador e segurança.
- Redirecionamento de URLs da web incorporadas em aplicativos quando não se deseja executar um navegador da web na sessão Citrix ou no cliente.

Requisitos do sistema

- VDAs de SO de sessão única ou multi-sessão
- Aplicativo Citrix Workspace™ para Windows

Navegadores:

- Internet Explorer 11
- Google Chrome com a Extensão de Redirecionamento de Navegador Citrix (disponível na Chrome Web Store do Google)
- Microsoft Edge (Chromium) com a Extensão de Redirecionamento de Navegador Citrix (disponível na Chrome Web Store do Google)

Configuração

O redirecionamento de conteúdo bidirecional deve ser habilitado usando a política Citrix tanto no VDA quanto no cliente para que o redirecionamento funcione. O redirecionamento de conteúdo bidirecional é desabilitado por padrão.

Para a configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações da política ICA.

Para a configuração do cliente, consulte Redirecionamento de conteúdo bidirecional na documentação do aplicativo Citrix Workspace para Windows.

As extensões do navegador devem ser registradas usando os comandos mostrados. Execute os comandos conforme necessário no VDA e no cliente, com base no navegador em uso.

Para registrar as extensões do navegador no VDA, abra um prompt de comando. Em seguida, execute `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` com a opção de navegador necessária, conforme mostrado nos exemplos:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Para registrar a extensão em todos os navegadores disponíveis, execute:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Para cancelar o registro de uma extensão de navegador, use a opção `/unreg<browser>` conforme mostrado no exemplo:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Para registrar as extensões do navegador no cliente, abra um prompt de comando e execute `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` com as mesmas opções dos exemplos mostrados.

> **Nota:**
>
> O comando de registro faz com que os navegadores Chrome e Edge solicitem aos usuários que ativem a Extensão de Redirecionamento de Navegador Citrix durante o primeiro lançamento. A extensão do navegador também pode ser instalada manualmente na Google Chrome Web Store.

Redirecionamento curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de curingas ao definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Citrix Studio, defina a URL curinga em **Allowed URLs to be redirected to Client**. O asterisco (*) é o caractere curinga.

> **NOTA:**
>
> - Não defina as **Allowed URLs to be redirected to VDA** na política do cliente. Certifique-se de que os sites definam as **Allowed URLs to be redirected to VDA** para evitar loops de redirecionamento infinitos.
> - Domínios de nível superior não são suportados. Por exemplo, `https://www.citrix.*` ou `http://www.citrix.co*` não é redirecionado.

Outras considerações

- Os requisitos e configurações do navegador são aplicáveis apenas ao navegador que inicia o redirecionamento. O navegador de destino, onde a URL é aberta após o redirecionamento ser bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, uma configuração de navegador suportada é necessária apenas no VDA. Por outro lado, ao redirecionar URLs do cliente para um VDA, uma configuração de navegador suportada é necessária apenas no cliente. As URLs redirecionadas são entregues ao navegador padrão configurado na máquina de destino, seja o cliente ou o VDA, dependendo da direção. O uso do mesmo tipo de navegador no VDA e no cliente NÃO é obrigatório.
- Verifique se as regras de redirecionamento não resultam em uma configuração em loop. Por exemplo, uma política de VDA é definida para redirecionar `https://www.citrix.com`, e a política do cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Apenas URLs de protocolo HTTP/HTTPS são suportadas. Encurtadores de URL não são suportados.
- O redirecionamento de cliente para VDA requer que o cliente Windows seja instalado com direitos de administrador.
- Se o navegador de destino já estiver aberto, a URL redirecionada é aberta em uma nova guia. Caso contrário, a URL é aberta em uma nova janela do navegador.
- O redirecionamento bidirecional de conteúdo não funciona quando o Acesso a Aplicativos Locais (LAA) está ativado.

Acesso a Aplicativos Locais e redirecionamento de URL

Introdução

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Com o Acesso a Aplicativos Locais, você pode:

- Acessar aplicativos instalados localmente em um laptop físico, PC ou outro dispositivo diretamente da área de trabalho virtual.
- Fornecer uma solução flexível de entrega de aplicativos. Se os usuários tiverem aplicativos locais que você não pode virtualizar ou que a TI não mantém, esses aplicativos ainda se comportarão como se estivessem instalados em uma área de trabalho virtual.

- Eliminar a latência de salto duplo quando os aplicativos são hospedados separadamente da área de trabalho virtual. Faça isso colocando um atalho para o aplicativo publicado no dispositivo Windows do usuário.
- Usar aplicativos como:
  - Software de videoconferência, como o GoToMeeting.
  - Aplicativos especializados ou de nicho que ainda não foram virtualizados.
  - Aplicativos e periféricos que, de outra forma, transfeririam grandes quantidades de dados de um dispositivo de usuário para um servidor e de volta para o dispositivo de usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops™, as sessões de área de trabalho hospedada usam o redirecionamento de URL para iniciar aplicativos de Acesso a Aplicativos Locais. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de bloqueio de URL do navegador) selecionando links incorporados em um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueio, o URL será aberto novamente na sessão da área de trabalho.

O redirecionamento de URL funciona apenas para sessões de área de trabalho, não para sessões de aplicativo. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo host-para-cliente, que é um tipo de redirecionamento FTA (Associação de Tipo de Arquivo) do servidor. Este FTA redireciona certos protocolos para o cliente, como HTTP, HTTPS, RTSP ou MMS. Por exemplo, se você abrir apenas links incorporados com HTTP, os links serão abertos diretamente com o aplicativo cliente. Não há suporte para lista de bloqueio ou lista de permissões de URL.

Quando o Acesso a Aplicativos Locais está ativado, os URLs exibidos aos usuários como links de aplicativos em execução localmente, de aplicativos hospedados pelo usuário ou como atalhos na área de trabalho são redirecionados de uma das seguintes maneiras:

- Do computador do usuário para a área de trabalho hospedada
- Do servidor Citrix Virtual Apps and Desktops para o computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento de conteúdo de sites específicos, configure a lista de permissões de URL e a lista de bloqueios de URL no Virtual Delivery Agent. Essas listas contêm chaves de registro de várias strings que especificam as configurações da política de

redirecionamento de URL. Para obter mais informações, consulte as configurações da política de Acesso a Aplicativos Locais.

As URLs podem ser renderizadas no VDA com as seguintes exceções:

- Informações de Geo/Localidade — Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na Geo). Por exemplo, se o VDA for provisionado de um data center no Reino Unido e o cliente estiver se conectando da Índia, o usuário espera ver in.msn.com. Em vez disso, o usuário vê uk.msn.com.
- Conteúdo multimídia — Sites que contêm conteúdo de mídia rica, quando renderizados no dispositivo cliente, proporcionam aos usuários finais uma experiência nativa e também economizam largura de banda, mesmo em redes de alta latência. Esse recurso redireciona sites com outros tipos de mídia, como Silverlight. Esse processo ocorre em um ambiente seguro. Ou seja, as URLs que o administrador aprova são executadas no cliente, enquanto o restante das URLs é redirecionado para o VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, ele deverá ter acesso ao arquivo para abri-lo. Portanto, você só pode abrir arquivos que residem em compartilhamentos de rede ou em unidades de cliente (usando o mapeamento de unidade de cliente) usando aplicativos locais. Por exemplo, ao abrir um arquivo PDF, se um leitor de PDF for um aplicativo local, o arquivo será aberto usando esse leitor de PDF. Como o aplicativo local pode acessar o arquivo diretamente, não há transferência de rede do arquivo via ICA® para abri-lo.

Requisitos, considerações e limitações

Oferecemos suporte ao Acesso a Aplicativos Locais nos sistemas operacionais válidos para VDAs para Windows Multi-session OS e para VDAs para Windows Single-session OS. O Acesso a Aplicativos Locais requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são suportados:

- Edge, versão mais recente
- Firefox, versão mais recente e versão de suporte estendido
- Chrome, versão mais recente

Revise as seguintes considerações e limitações ao usar o Acesso a Aplicativos Locais e o redirecionamento de URL.

- O Acesso a Aplicativos Locais foi projetado para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o Acesso a Aplicativos Locais com um desktop virtual que é executado no modo de janela ou não cobre todos os monitores.
  - Vários monitores — Quando um monitor é maximizado, ele se torna o desktop padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo que os aplicativos subsequentes normalmente iniciem em outro monitor.
  - O recurso suporta um VDA. Não há integração com múltiplos VDAs simultâneos.
- Alguns aplicativos podem se comportar de forma inesperada, afetando os usuários:
  - As letras das unidades podem confundir os usuários, como C: local em vez da unidade C: da área de trabalho virtual.
  - As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
  - Aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados no cliente.
  - Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).
  - Aplicativos locais aparecem com o tema do Windows da máquina local.
  - Aplicativos em tela cheia não são suportados. Esses aplicativos incluem aplicativos que abrem em tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem a área de trabalho inteira.
  - O Acesso a Aplicativos Locais copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e no menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
  - Aplicativos que personalizam como a ordem das janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
  - Atalhos não são suportados, incluindo Meu Computador, Lixeira, Painel de Controle, atalhos de Unidade de Rede e atalhos de pasta.
  - Os seguintes tipos de arquivo e arquivos não são suportados: tipos de arquivo personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
  - O agrupamento da barra de tarefas não é suportado para aplicativos hospedados no cliente ou VDA mistos de 32 bits e 64 bits. Ou seja, agrupar aplicativos locais de 32 bits com aplicativos VDA de 64 bits.

  - Aplicativos não podem ser iniciados usando COM. Por exemplo, se você clicar em um documento do Office incorporado de dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local falhará.

- Cenários de salto duplo, onde um usuário está iniciando uma área de trabalho virtual de dentro de outra sessão de área de trabalho virtual, não são suportados.
- O redirecionamento de URL suporta apenas URLs explícitas (ou seja, URLs que aparecem na barra de endereços do navegador ou encontradas usando a navegação no navegador, dependendo do navegador).
- O redirecionamento de URL funciona apenas com sessões de desktop, não com sessões de aplicativo.
- A pasta de desktop local em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução localmente se comportam de acordo com as configurações da barra de tarefas estabelecidas para o desktop virtual. No entanto, os atalhos para aplicativos em execução localmente não são agrupados com instâncias em execução desses aplicativos. Eles também não são agrupados com instâncias em execução de aplicativos hospedados ou atalhos fixados para aplicativos hospedados. Os usuários podem fechar apenas janelas de aplicativos em execução localmente a partir da Barra de Tarefas. Embora os usuários possam fixar janelas de aplicativos locais na Barra de Tarefas e no menu Iniciar do desktop, os aplicativos podem não iniciar de forma consistente ao usar esses atalhos.
- Se você definir a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**, o redirecionamento de conteúdo do navegador não é suportado. Por padrão, o Acesso a Aplicativos Locais é proibido.

Interação com o Windows

A interação do Acesso a Aplicativos Locais com o Windows inclui os seguintes comportamentos.

- Comportamento de atalho do Windows 8 e Windows Server 2012

  - Os aplicativos da Windows Store instalados no cliente não são enumerados como parte dos atalhos do Acesso a Aplicativos Locais.
  - Arquivos de imagem e vídeo são abertos por padrão usando aplicativos da Windows Store. No entanto, o Acesso a Aplicativos Locais enumera os aplicativos da Windows Store e abre atalhos com aplicativos de desktop.

- Programas Locais

  - Para o Windows 7, a pasta está disponível no menu Iniciar.
  - Para o Windows 8, Programas Locais está disponível apenas quando o usuário escolhe **Todos os Aplicativos** como uma categoria na tela Iniciar. Nem todas as subpastas são exibidas em Programas Locais.

- Recursos gráficos do Windows 8 para aplicativos
  - Os aplicativos de desktop são restritos à área de trabalho e são cobertos pela tela Iniciar e aplicativos estilo Windows 8.
  - Os aplicativos de Acesso a Aplicativos Locais não se comportam como aplicativos de desktop no modo de vários monitores. No modo de vários monitores, a tela Iniciar e a área de trabalho são exibidas em monitores diferentes.
- Windows 8 e Redirecionamento de URL de Acesso a Aplicativos Locais
  - Como o Internet Explorer do Windows 8 não tem complementos habilitados, use o Internet Explorer da área de trabalho para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desabilita os complementos por padrão. Para implementar o Redirecionamento de URL, desabilite a configuração aprimorada do Internet Explorer. Em seguida, redefina as opções do Internet Explorer e reinicie para garantir que os complementos estejam habilitados para usuários padrão.

Configurar Acesso a Aplicativos Locais e redirecionamento de URL

Para usar o Acesso a Aplicativos Locais e o redirecionamento de URL com o aplicativo Citrix Workspace™:

- Instale o aplicativo Citrix Workspace na máquina cliente local. Você pode habilitar ambos os recursos durante a instalação do aplicativo Citrix Workspace ou pode habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo.
- Defina a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**. Você também pode configurar as configurações de política de lista de permissões e lista de bloqueios de URL para redirecionamento de URL. Para obter mais informações, consulte Configurações de política de Acesso a Aplicativos Locais.

Habilitar Acesso a Aplicativos Locais e redirecionamento de URL

Para habilitar o Acesso a Aplicativos Locais para todos os aplicativos locais, siga estas etapas:

1. Inicie o Citrix Studio.

- Para implantações locais, abra o **Citrix Studio** no **menu Iniciar**.
- Para implantações de serviço em nuvem, vá para **Citrix Cloud™ > Serviço Virtual Apps and Desktops > guia Gerenciar**.

2. No painel de navegação do Studio, clique em **Políticas**.
3. No painel Ações, clique em **Criar Política**.
4. Na janela Criar Política, digite “Permitir Acesso a Aplicativos Locais” na caixa de pesquisa e clique em **Selecionar**.
5. 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.
6. Na janela Criar Política, digite “lista de permissões de redirecionamento de URL” na caixa de pesquisa e clique em **Selecionar**. A lista de permissões de redirecionamento de URL especifica as URLs a serem abertas no navegador padrão da sessão remota.
7. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
8. Na janela Criar Política, digite “lista de bloqueio de redirecionamento de URL” na caixa de pesquisa e, em seguida, clique em **Selecionar**. A lista de bloqueio de redirecionamento de URL especifica os URLs que são redirecionados para o navegador padrão em execução no endpoint.
9. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
10. Na página Configurações, clique em **Avançar**.
11. Na página Usuários e Máquinas, atribua a política aos Grupos de Entrega aplicáveis e, em seguida, clique em **Avançar**.
12. 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. Para obter mais informações, consulte Configurando o modelo administrativo do Objeto de Política de Grupo.
- Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Modelos Administrativos > Componentes Citrix > Citrix Workspace** somente quando você adiciona o CitrixBase.admx/CitrixBase.adml à pasta %systemroot%\policyDefinitions.

Para habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá para **Configuração do Computador > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Clique em **Configurações de Acesso a Aplicativos Locais**.
4. Selecione **Habilitado** e, em seguida, selecione **Permitir Redirecionamento de URL**. Para redirecionamento de URL, registre os complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais adiante neste artigo.

Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o SDK do PowerShell.

Para o Editor do Registro, consulte O Acesso a Aplicativos Locais para aplicativos publicados na lista de recursos gerenciados através do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina onde o Delivery Controller™ está sendo executado.
2. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Para ter acesso a **Adicionar Aplicativo de Acesso a Aplicativos Locais** em uma implantação de serviço 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. Abra o **Citrix Studio** no menu **Iniciar**.
2. No painel de navegação do Studio, clique em **Aplicativos**.
3. 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** no painel Ações. Para exibir a opção Adicionar Aplicativo de Acesso a Aplicativos Locais no painel Ações, clique em **Atualizar**.
4. 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 depois clique em **Avançar**. Você pode especificar o ícone para o aplicativo selecionado. Você também pode especificar se o atalho para o aplicativo local na área de trabalho virtual é visível no menu Iniciar, na área de trabalho ou em ambos.
- Na página Resumo, revise as configurações e, em seguida, clique em **Finish** para sair do assistente de Acesso a Aplicativos Locais.

Registrar complementos do navegador

> **Nota:**
>
> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente quando você instala o aplicativo Citrix Workspace pela 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 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 usam as opções da Internet ou os complementos no prompt estiverem desabilitados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam as URLs.

Quando um complemento é instalado, o Firefox solicita que você permita ou impeça a instalação do complemento em uma nova página de guia. Permita o complemento para que o recurso funcione.

- O complemento do Chrome sempre redireciona a URL final para a qual se navega, e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desativa a extensão, o recurso de redirecionamento de URL não funciona no Chrome. Se o redirecionamento de URL for necessário no modo de navegação anônima, permita que a extensão seja executada nesse modo nas configurações do navegador.

Configurar o comportamento do aplicativo local ao fazer logoff e desconectar

Nota:

Se você não seguir estas etapas para configurar as definições, por padrão, os aplicativos locais continuarão a ser executados quando um usuário fizer logoff ou se desconectar da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.

Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, consulte Comportamento do aplicativo local ao fazer logoff e desconectar na lista de recursos gerenciados por meio do registro.

Redirecionamento USB genérico e considerações sobre unidades de cliente

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes com alta latência ou sensíveis à segurança.

A tecnologia HDX oferece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde este é inadequado, por exemplo:

- O dispositivo USB possui recursos mais avançados que não fazem parte do suporte otimizado, como um mouse ou webcam com mais botões.
- Os usuários precisam de funções que não fazem parte do suporte otimizado.
- O dispositivo USB é um dispositivo especializado, como equipamento de teste e medição ou um controlador industrial.
- Um aplicativo requer acesso direto ao dispositivo como um dispositivo USB.
- O dispositivo USB tem apenas um driver Windows disponível. Por exemplo, um leitor de cartão inteligente pode não ter um driver disponível para o aplicativo Citrix Workspace™ para Android.
- A versão do aplicativo Citrix Workspace não oferece suporte otimizado para este tipo de dispositivo USB.

Com o redirecionamento USB genérico:

- Os usuários não precisam instalar drivers de dispositivo no dispositivo do usuário.
- Os drivers de cliente USB são instalados na máquina VDA.

Importante:

- O redirecionamento USB genérico pode ser usado em conjunto com o suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as configurações de política de dispositivos USB do Citrix para redirecionamento USB genérico e suporte otimizado.
- A configuração de política do Citrix em Regras de otimização de dispositivo USB do cliente é uma configuração específica para redirecionamento USB genérico, para um dispositivo USB específico. Ela não se aplica ao suporte otimizado conforme descrito aqui.

Considerações de desempenho para dispositivos USB

A latência da rede e a largura de banda podem afetar a experiência do usuário e a operação do dispositivo USB ao usar o redirecionamento USB genérico para alguns tipos de dispositivos USB. Por exemplo, dispositivos sensíveis ao tempo podem não funcionar corretamente em links de alta latência e baixa largura de banda. Use o suporte otimizado em vez disso, sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para serem utilizáveis, por exemplo, um mouse 3D (usado com aplicativos 3D que também geralmente exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você poderá mitigar o problema ajustando o uso da largura de banda de outros componentes usando as configurações da política de largura de banda. Para obter mais informações, consulte Configurações da política de largura de banda para redirecionamento de dispositivo USB do cliente e Configurações da política de conexão multi-stream.

Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartão inteligente, leitores de impressão digital e mesas digitalizadoras de assinatura. Outros dispositivos USB, como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser confidenciais.

Importante:

Não use o redirecionamento USB genérico para leitores de cartão inteligente. Essa funcionalidade é desabilitada por padrão para leitores de cartão inteligente e não é suportada se ativada.

Dispositivos USB são frequentemente usados para distribuir malware. A configuração do Citrix Workspace app e do Citrix Virtual Apps and Desktops™ pode reduzir, mas não eliminar, o risco desses dispositivos USB. Essa situação se aplica independentemente de ser usado o redirecionamento USB genérico ou o suporte otimizado.

Importante:

Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX usando TLS ou IPsec.

Habilite o suporte apenas para os dispositivos USB de que você precisa. Configure o redirecionamento USB genérico e o suporte otimizado para atender a essa necessidade.

Forneça orientação aos usuários para o uso seguro de dispositivos USB:

- Use apenas dispositivos USB obtidos de uma fonte confiável.
- Não deixe dispositivos USB sem 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 oferecem suporte ao redirecionamento USB genérico:

- Citrix Workspace app para Windows, consulte Configurando a entrega de aplicativos.
- Citrix Workspace app para Mac, consulte Citrix Workspace app 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 de VDA para SO de sessão única, da versão 7.6 até a atual.

O redirecionamento genérico de USB é compatível com sessões de desktop de VDA para SO de múltiplas sessões, da versão 7.6 até a atual, com estas restrições:

- O VDA deve estar executando o Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o Host da Sessão da Área de Trabalho Remota (RDSH) para o SO do VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não são compatíveis com o redirecionamento genérico de USB porque não seria útil redirecioná-los:

- Modems USB.
- Adaptadores de rede USB.
- Hubs USB. Os dispositivos USB conectados aos hubs USB são tratados individualmente.
- Portas COM virtuais USB. Use o redirecionamento de porta COM em vez do redirecionamento genérico de USB.

Para obter informações sobre dispositivos USB que foram testados com redirecionamento USB genérico, consulte Citrix Ready Marketplace. Alguns dispositivos USB não funcionam corretamente com o redirecionamento USB genérico.

Configurar o redirecionamento USB genérico

Você pode controlar e configurar separadamente quais tipos de dispositivos USB usam o redirecionamento USB genérico:

- No VDA, usando as configurações de política do Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações de política de dispositivos USB na referência de configurações de política
- No aplicativo Citrix Workspace, usando mecanismos dependentes do aplicativo Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações de registro que configuram o aplicativo Citrix Workspace para Windows. Por padrão, o redirecionamento USB é permitido para certas classes de dispositivos USB e negado para outras. Para obter mais informações, consulte Configurar na documentação do aplicativo Citrix Workspace para Windows.

Esta configuração separada oferece flexibilidade. Por exemplo:

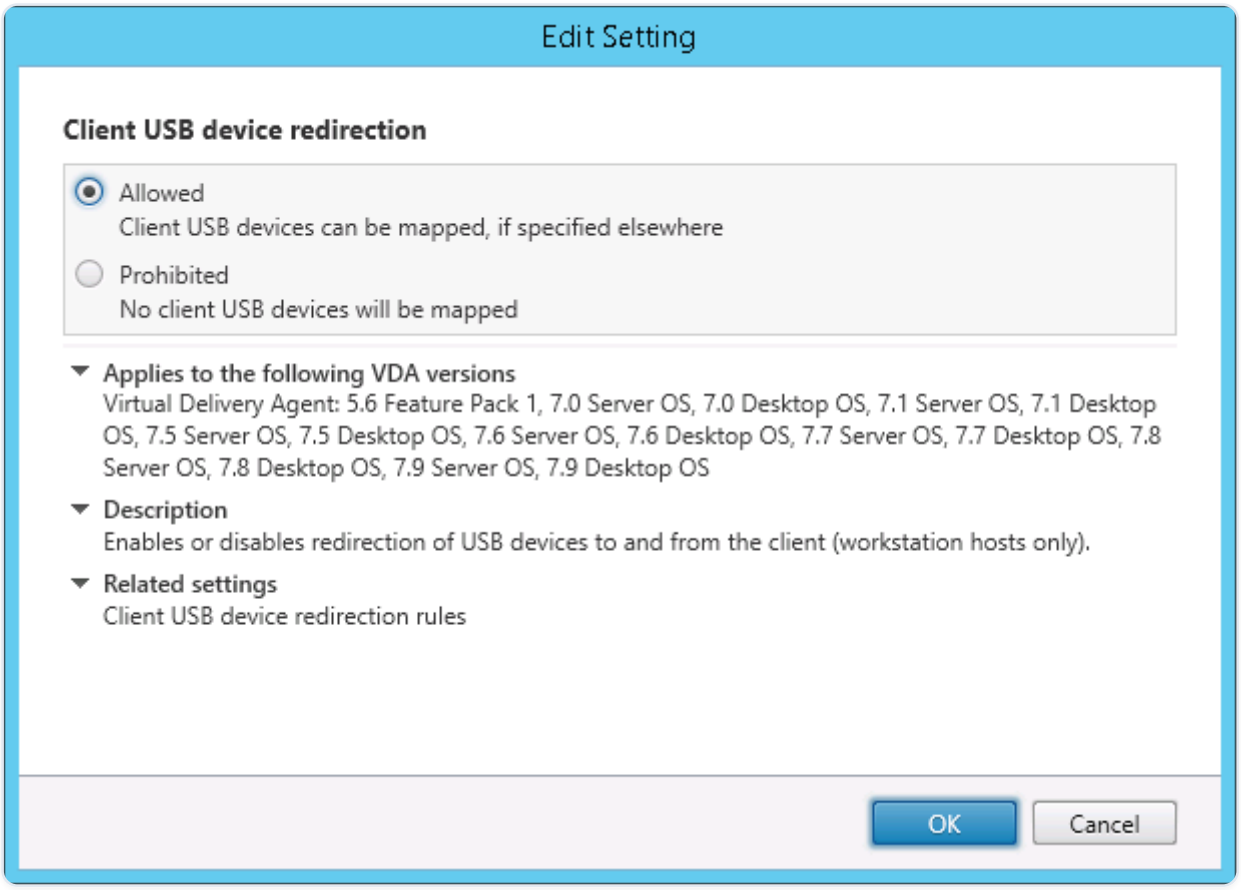
- Se duas organizações ou departamentos diferentes forem responsáveis pelo aplicativo Citrix Workspace e pelo VDA, eles poderão impor o controle separadamente. Essa configuração se aplica quando um usuário em uma organização acessa um aplicativo em outra organização.
- As configurações de política do 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 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:

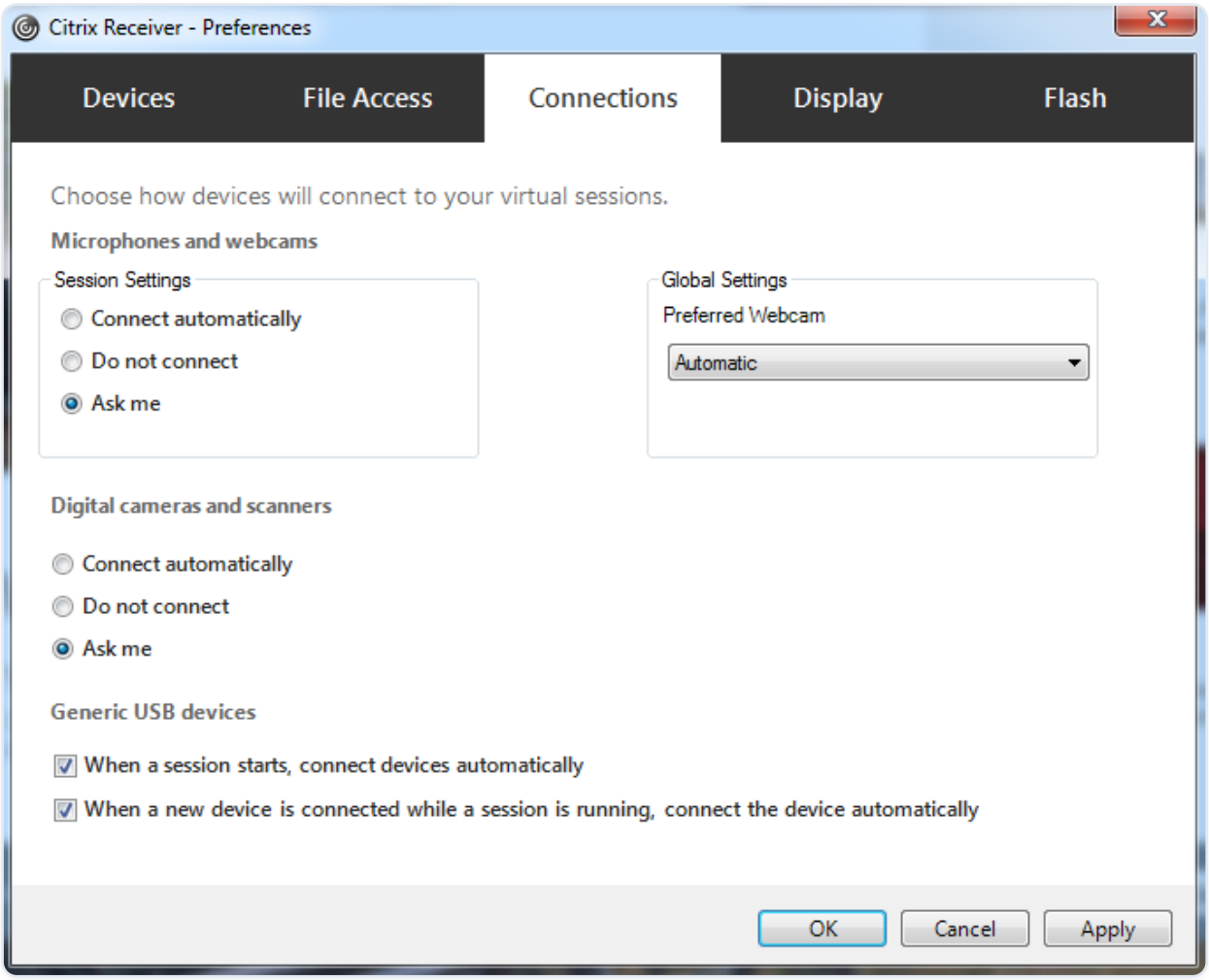
1. Adicione o Redirecionamento de dispositivo USB do cliente a uma política e defina seu valor como **Permitido**.



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**.



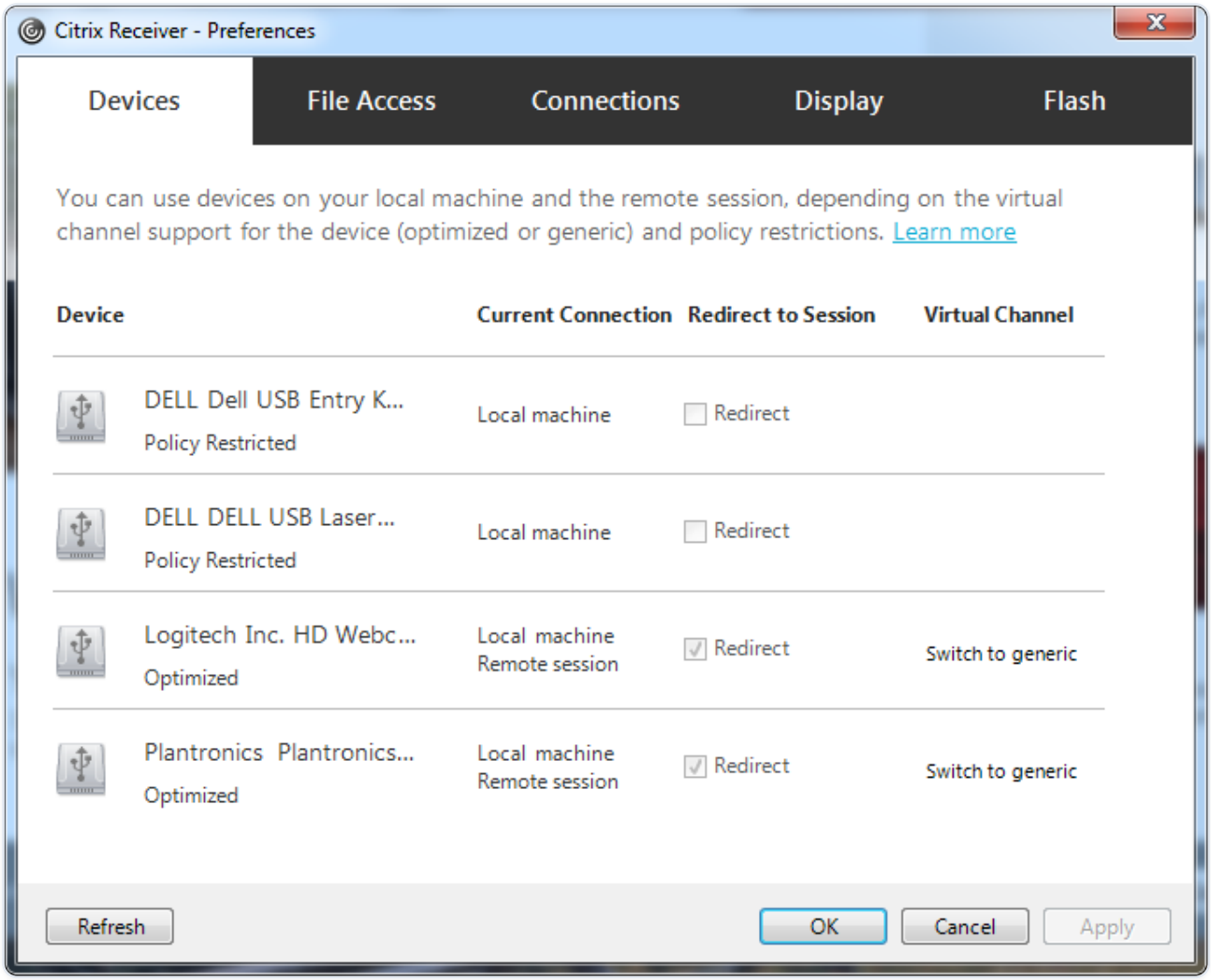
Se você especificou as regras de política USB para o VDA na etapa anterior, especifique as mesmas regras de política para o aplicativo Citrix Workspace.

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 **Alternar para genérico** na guia Dispositivos da caixa de diálogo Preferências.
- Selecione automaticamente o dispositivo USB para usar o redirecionamento USB genérico, configurando o redirecionamento automático para o tipo de dispositivo USB (por exemplo, AutoRedirectStorage=1) e defina as configurações de preferência do usuário USB para conectar dispositivos USB automaticamente. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

> **Observação:**
>
> Configure o redirecionamento USB genérico para uso com uma webcam somente se a webcam for considerada incompatível com o redirecionamento multimídia HDX.

> Para evitar que dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e o VDA.

Para 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 Console de Gerenciamento de Política de Grupo do Citrix (`CitrixGroupPolicyManagement_x64.msi`) e instale-o em seu sistema Active Directory e, em seguida, gerencie as políticas de grupo do AD. (Não instale o MSI em um VDA.)
- Para o Citrix Workspace app para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: raiz do dvd `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops no local:

- Para o VDA, edite as regras de substituição do administrador para as máquinas do SO de várias sessões por meio de regras de política de grupo. O Console de Gerenciamento de Política de Grupo está incluído na mídia de instalação:
  - 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 os Códigos de Classe USB disponíveis
Subclasse	Subclasse do descritor do dispositivo ou de um descritor de interface
Prot	Protocolo do descritor do dispositivo ou de um descritor de interface

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por `#`. Um delimitador não é necessário, e o comentário é ignorado para fins de correspondência.
- Linhas em branco e linhas de comentário puro são ignoradas.
- Espaços em branco são usados como separador, 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:**

> Se você estiver usando o arquivo de modelo ADM, você deve criar regras em uma única linha, como uma lista separada por ponto e vírgula.

> Exemplos:

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para identificadores de fornecedor e produto:

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para uma classe, subclasse e protocolo definidos:

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

Usar e remover dispositivos USB

Os usuários podem conectar um dispositivo USB antes ou depois de iniciar uma sessão virtual.

Ao usar o Citrix Workspace app para Windows, o seguinte se aplica:

- Dispositivos conectados após o início de uma sessão aparecem imediatamente no menu USB do Desktop Viewer.
- Se um dispositivo USB não estiver sendo redirecionado corretamente, você pode tentar resolver o problema esperando para conectar o dispositivo até depois que a sessão virtual for iniciada.
- Para evitar perda de dados, use o ícone "Remover Hardware com Segurança" do Windows antes de remover o dispositivo USB.

Controles de segurança para dispositivos de armazenamento em massa USB

É fornecido suporte otimizado para dispositivos de armazenamento em massa USB. Este suporte faz parte do mapeamento de unidades cliente do Citrix Virtual Apps and Desktops. As unidades no dispositivo do usuário são mapeadas automaticamente para letras de unidade na área de trabalho virtual quando os usuários fazem logon. As unidades são exibidas como pastas compartilhadas que 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 o dispositivo durante uma sessão	Não	Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura

Se o redirecionamento USB genérico e as políticas de mapeamento de unidades 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 unidades cliente. Quando o redirecionamento USB genérico e as políticas de mapeamento de unidades cliente estiverem habilitados 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.

Controlar o acesso a arquivos com o mapeamento de unidades cliente

Você pode controlar se os usuários podem copiar arquivos de seus ambientes virtuais para seus dispositivos de usuário. Por padrão, arquivos e pastas em unidades cliente mapeadas estão disponíveis no modo de leitura/gravação dentro da sessão.

Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, habilite a configuração de política **Acesso somente leitura à unidade cliente**. Ao adicionar esta configuração a uma política, certifique-se de que a configuração de redirecionamento de unidade cliente esteja definida como **Permitido** e também seja adicionada à política.

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 impressão:

- Os tipos de provisionamento de impressora disponíveis
- Como os trabalhos de impressão são roteados
- Os fundamentos do gerenciamento de drivers de impressora

Os conceitos de impressão são baseados nos conceitos de impressão do Windows. Para configurar e gerenciar com sucesso a impressão em seu ambiente, você deve entender como a impressão de rede e cliente do Windows funciona e como isso se traduz em comportamento de impressão neste ambiente.

Processo de impressão

Neste ambiente, toda a impressão é iniciada (pelo usuário) nas máquinas que hospedam aplicativos. Os trabalhos de impressão são redirecionados através do servidor de impressão de rede ou dispositivo do usuário para o dispositivo de impressão.

Não há 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 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. Esta 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.

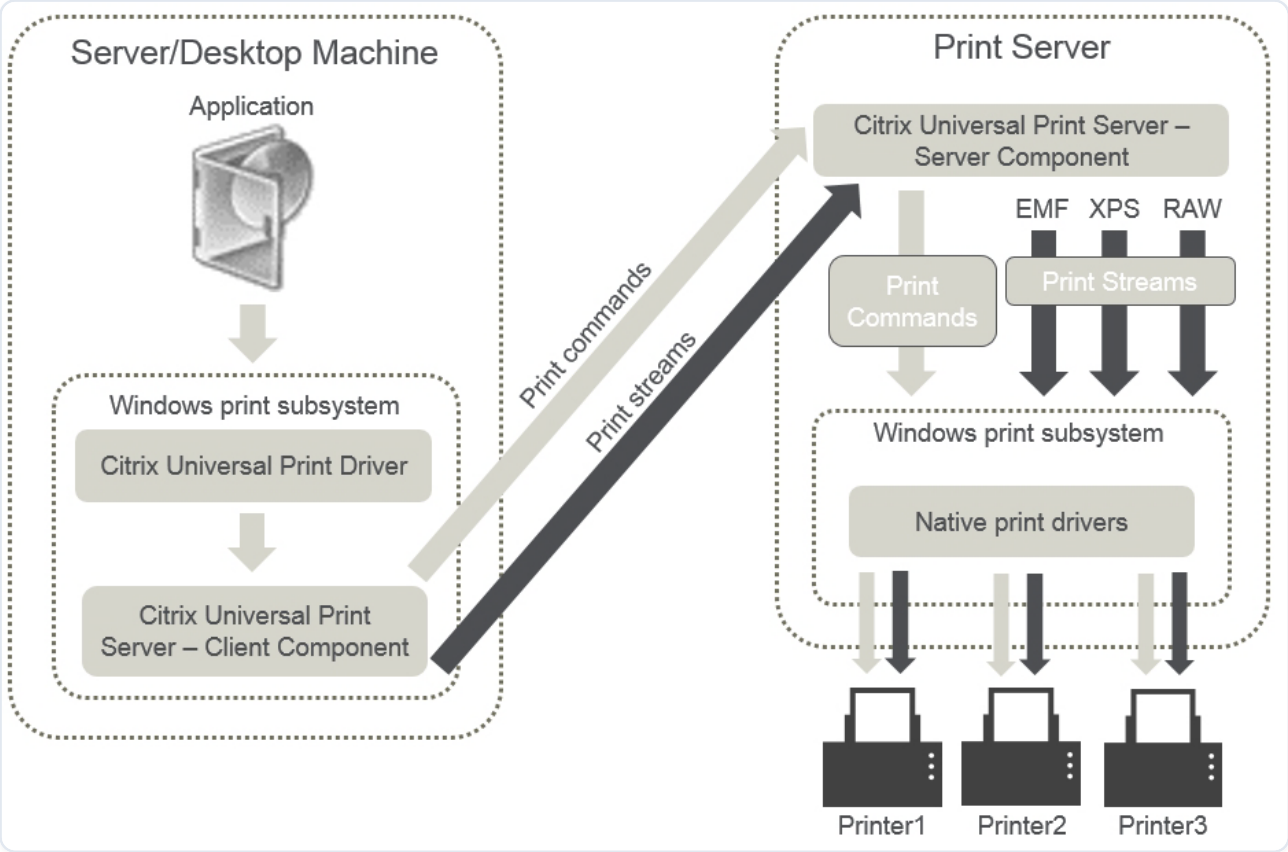
O recurso Universal Print Server compreende:

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.



Quando você habilita 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 automaticamente todas as impressoras no dispositivo do usuário, 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.

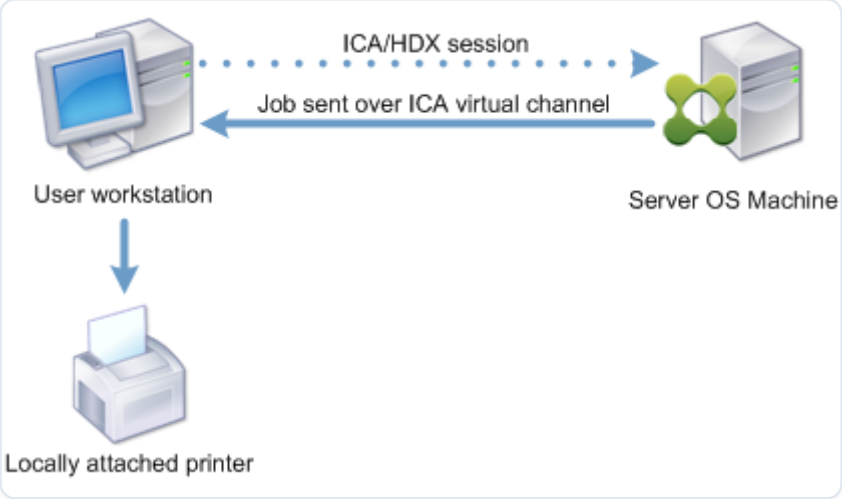
Roteamento de trabalhos de impressão

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 enfileirados. Ambos os aspectos desse conceito são importantes. O roteamento afeta o tráfego de rede. O enfileiramento afeta a utilização de recursos locais no dispositivo que processa o trabalho.

Nesse ambiente, os trabalhos de impressão podem seguir dois caminhos para um dispositivo de impressão: através do cliente ou através de um servidor de impressão de rede. Esses caminhos são chamados de caminho de impressão do cliente e caminho de impressão de rede. Qual caminho é escolhido por padrão depende do tipo de impressora usada.

Impressoras conectadas localmente

O sistema roteia os 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 do trabalho de impressão. Quando um dispositivo de impressão é conectado localmente ao dispositivo do usuário, os trabalhos de impressão são roteados pelo canal virtual ICA.



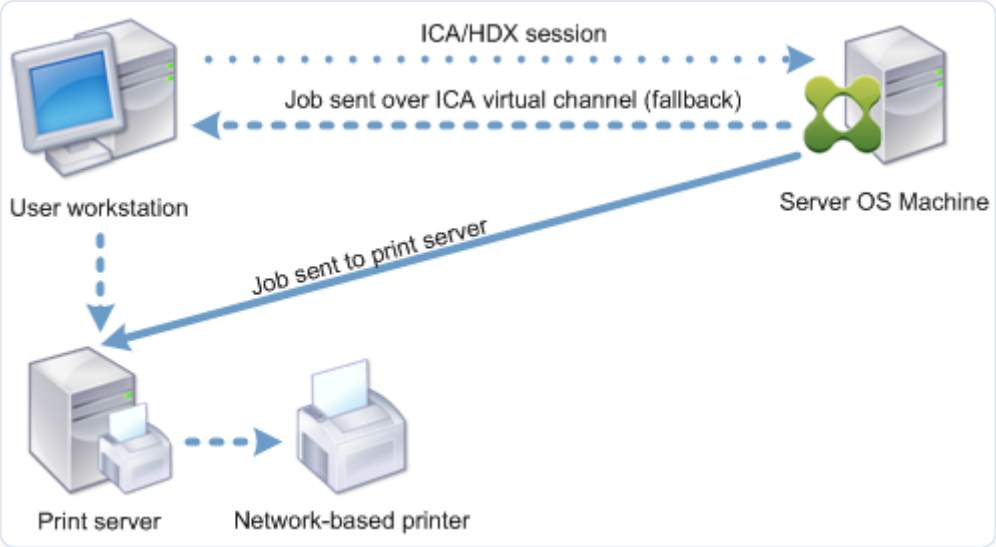
Impressoras baseadas em rede

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina do SO de múltiplas sessões, através da rede e diretamente para o servidor de impressão. No entanto, os trabalhos de impressão são roteados automaticamente pela conexão ICA nas seguintes situações:

- Se o desktop virtual ou aplicativo não conseguir entrar em contato com o servidor de impressão.
- Se o driver de impressora nativo não estiver disponível na máquina do SO de múltiplas sessões.

Se o Servidor de Impressão Universal 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 compactação de tráfego que resultam 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 clientes leves 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 "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.

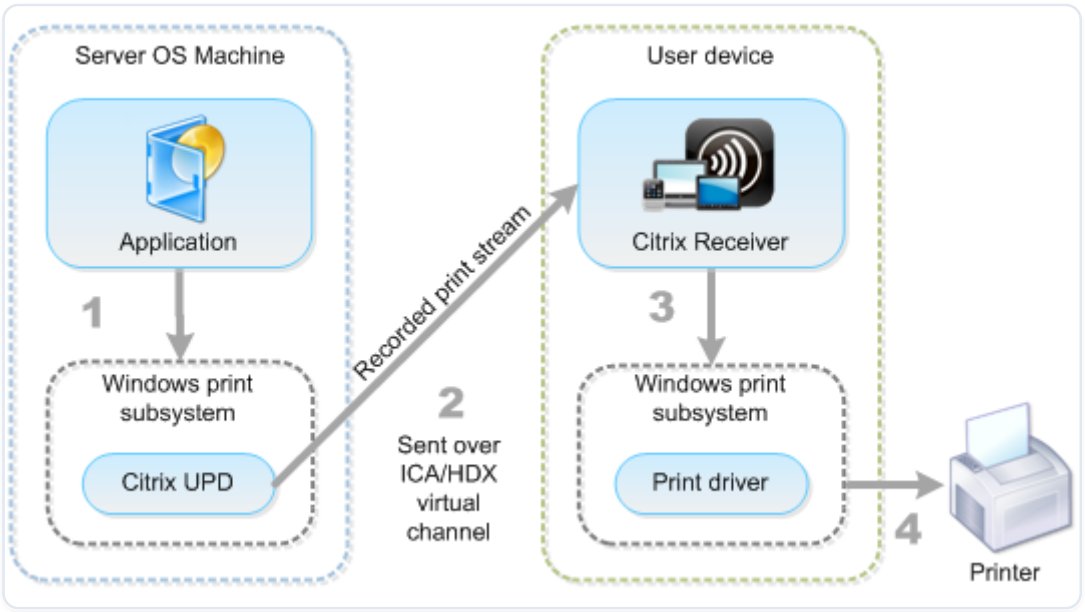
O Citrix UPD oferece suporte aos seguintes formatos de impressão:

- Formato de Meta-arquivo Aprimorado (**EMF**), padrão. EMF é a versão de 32 bits do formato Windows Metafile (WMF). O driver EMF só pode ser usado por clientes baseados em Windows.
- Especificação de Papel XML (**XPS**). O driver XPS usa XML para criar um "papel eletrônico" independente de plataforma, semelhante ao formato Adobe PDF.
- Linguagem de Comando de Impressora (**PCL5c** e **PCL4**). PCL é um protocolo de impressão desenvolvido originalmente pela Hewlett-Packard para impressoras a jato de tinta. É usado para imprimir texto e gráficos básicos e é amplamente suportado em periféricos multifuncionais e HP LaserJet.
- PostScript (**PS**). PostScript é uma linguagem de computador que pode ser usada para imprimir texto e gráficos vetoriais. O driver é amplamente utilizado em impressoras de baixo custo e periféricos multifuncionais.

Os drivers PCL e PS são mais adequados ao usar dispositivos não baseados em Windows, como um cliente Mac ou UNIX. A ordem em que o Citrix UPD tenta usar os drivers pode ser alterada usando a configuração de política preferência de driver universal.

O Citrix UPD (drivers EMF e XPS) oferece suporte a recursos avançados de impressão, como grampeamento e seleção de origem do papel. Esses recursos estão disponíveis se o driver nativo os disponibilizar usando a tecnologia Microsoft Print Capability. O driver nativo deve usar as Palavras-chave do Esquema de Impressão padronizadas no XML de Recursos de Impressão. Se forem usadas palavras-chave não padronizadas, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

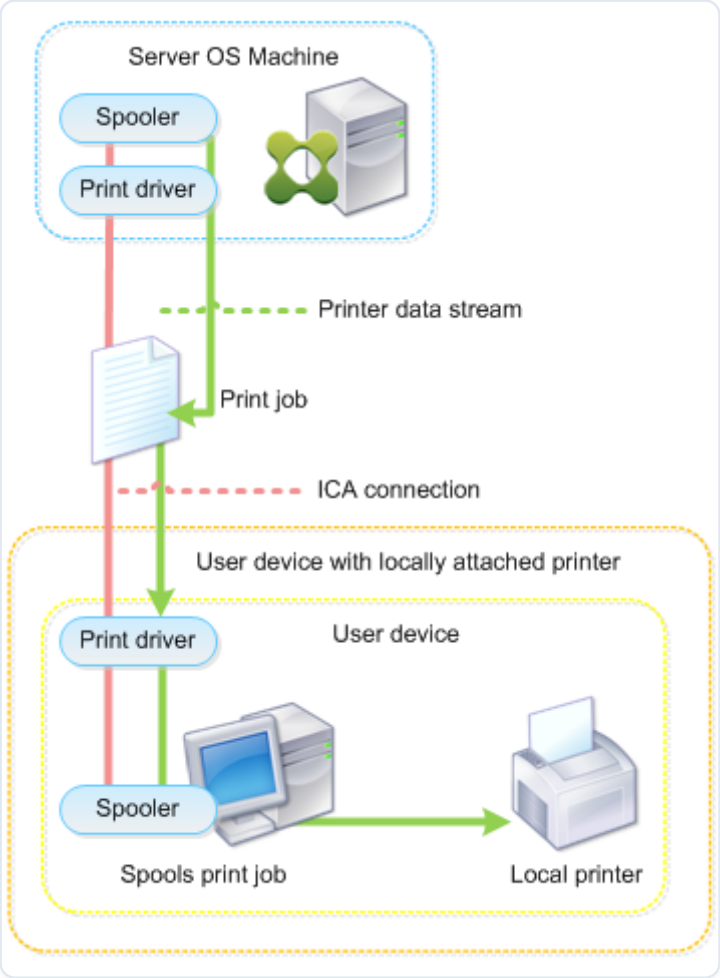
A ilustração a seguir mostra os componentes do driver de impressão universal e um fluxo de trabalho típico para uma impressora conectada localmente a um dispositivo.



Ao planejar sua estratégia de gerenciamento de drivers, determine se você oferecerá suporte ao driver de impressão universal, a drivers específicos do dispositivo ou a ambos. Se você oferece suporte a drivers padrão, deve determinar:

Durante a autocriação da impressora, se o sistema detectar uma nova impressora local conectada a um dispositivo de usuário, ele verificará a máquina do SO de várias sessões em busca do driver de impressora necessário. Por padrão, se um driver nativo do Windows não estiver disponível, o sistema usará o driver de impressão universal.

O driver da impressora na máquina do SO de múltiplas sessões e o driver no dispositivo do usuário devem corresponder para que a impressão seja bem-sucedida. A ilustração a seguir mostra como um driver de impressora é usado em dois locais para impressão do cliente.



- Os tipos de drivers a serem suportados.
- Se deve instalar drivers de impressora automaticamente quando eles estiverem ausentes das máquinas do SO de múltiplas sessões.
- Se deve criar listas de compatibilidade de drivers.

Conteúdo relacionado

- Exemplo de configuração de impressão
- Melhores práticas, considerações de segurança e operações padrão
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

Exemplo de configuração de impressão

Escolher as opções de configuração de impressão mais apropriadas para suas necessidades e ambiente pode simplificar a administração. Embora a configuração de impressão padrão permita que os usuários imprimam na maioria dos ambientes, as configurações padrão podem não fornecer a experiência de usuário esperada ou o uso ideal da rede e a sobrecarga de gerenciamento para seu ambiente.

Sua configuração de impressão depende de:

- Suas necessidades de negócios e sua infraestrutura de impressão existente.

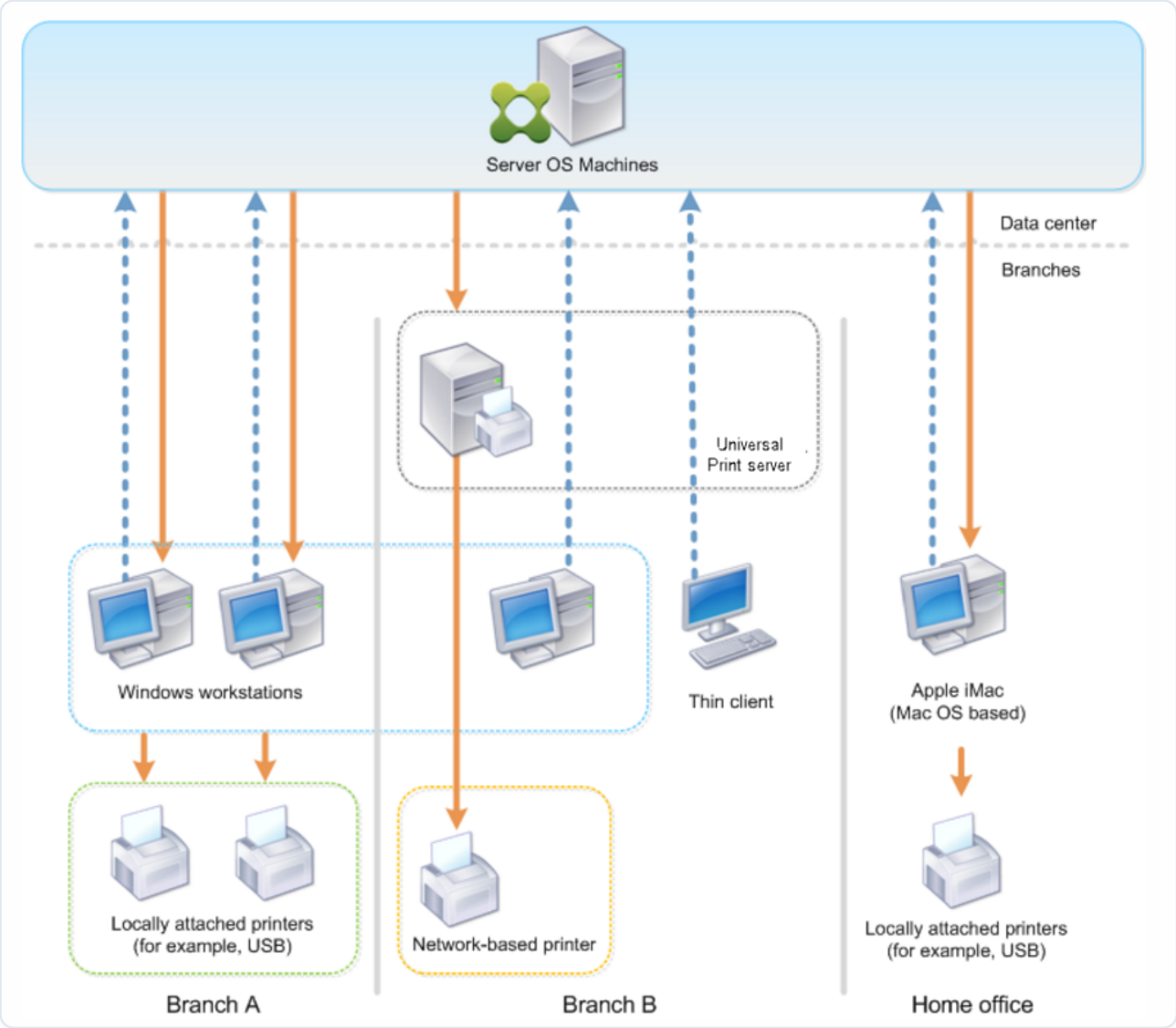
  Projete sua configuração de impressão em torno das necessidades da sua organização. Sua implementação de impressão existente (se os usuários podem adicionar impressoras, quais usuários têm acesso a quais impressoras e assim por diante) pode ser um guia útil ao definir sua configuração de impressão.
- Se sua organização possui políticas de segurança que reservam impressoras para determinados 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 oferecer aos usuários a mesma experiência em uma sessão que eles teriam 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 área de trabalho 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 área de trabalho 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 área de trabalho virtual ou aplicativo, as impressoras configuradas localmente são enumeradas por meio de autocriação. A área de trabalho 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 área de trabalho 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 local do driver da impressora (de acordo com o modelo de administração delegada).

Se uma fila de impressão precisar ser modificada ou adicionada, os administradores Citrix devem modificar a respectiva política de impressora de sessão dentro do ambiente.

Como o tráfego de impressão de rede será enviado fora do canal virtual ICA, o QoS é implementado. O tráfego de rede de entrada e saída nas portas usadas pelo tráfego ICA/HDX é priorizado sobre todo o outro tráfego de rede. Essa configuração garante que as sessões 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 de 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 de 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 Multi-session OS.
- Use o mapeamento de driver 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 driver de impressora para evitar que impressoras sejam criadas com o driver.
- Tente evitar o uso de drivers de modo kernel versão 2.
- Para determinar se um modelo de impressora é compatível, 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 o Terminal Services 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 Terminal Services pelo programa Windows Hardware Quality Labs (WHQL). A Citrix não certifica drivers de impressora.

Considerações de segurança

As soluções de impressão da Citrix são seguras por design.

- O Citrix Print Manager Service 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 para a 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 será o seguinte:

- O Universal Print Server está desativado.
- 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 desativar 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 "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.

- Todas as impressoras configuradas no dispositivo do usuário são criadas automaticamente no início de cada sessão.

  Esse 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, através do 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.

  Esse comportamento é equivalente a desativar 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 essa operação, o sistema armazenará as propriedades de impressão em perfis de usuário na máquina Multi-session OS.

  Esse 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 posterior, 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 de impressora se estiver disponível na máquina Multi-session OS. Se o driver de 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 configuração de política do Citrix "Instalação automática de drivers de impressora embutidos" e configurar a configuração de impressão Universal com "Usar impressão universal somente se o driver solicitado não estiver disponível".

Habilitar a "Instalação automática de drivers de impressora embutidos" pode resultar na instalação de um grande número de drivers de impressora nativos.

Nota:

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 as políticas Citrix® para especificar:

- Como as impressoras são provisionadas (ou adicionadas a sessões)
- Como os trabalhos de impressão são roteados
- Como os drivers de impressora são gerenciados

Você pode ter diferentes configurações de impressão para diferentes dispositivos de usuário, usuários ou quaisquer outros objetos nos quais as políticas são filtradas.

A maioria das funções de impressão é configurada por meio das configurações de política de impressão do Citrix. As configurações de impressão seguem o comportamento padrão da política Citrix.

O sistema pode gravar as configurações da impressora no objeto da impressora no final de uma sessão ou em um dispositivo de impressão cliente, desde que a conta de rede do usuário tenha permissões suficientes. Por padrão, o aplicativo Citrix Workspace™ usa as configurações armazenadas no objeto da impressora na sessão, antes de procurar em outros locais por configurações e preferências.

Por padrão, o sistema armazena, ou retém, as propriedades da impressora no dispositivo do usuário (se suportado pelo dispositivo) ou no perfil do usuário na máquina do SO multi-sessão. 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 selecionada como orientação da página, paisagem será salva 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 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 orientação da página e o nome da impressora, dentro do documento. Essas configurações aparecem por padrão na próxima vez que você imprimir esse documento.
- **De alterações feitas por um usuário durante uma sessão** - O sistema mantém apenas as alterações nas configurações de impressão de uma impressora criada automaticamente se a alteração foi feita no Painel de Controle na sessão; ou seja, na máquina do SO multi-sessão.
- **Na máquina do SO multi-sessão** - 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 de várias sessões 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 retorna ao perfil do usuário na máquina do sistema operacional de várias sessões.

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 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 oferece suporte às 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 Multi-session OS que permite impressão local ou em rede 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 Servidor de Impressão Universal, instale o componente UpsServer em seus servidores de impressão, conforme descrito nos documentos de instalação, e configure-o. Para obter mais informações, consulte Instalar componentes principais e Instalar usando a linha de comando.

Para ambientes onde você deseja implantar o componente UPClient separadamente, por exemplo, com **XenApp 6.5**:

1. Baixe o pacote autônomo do Citrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) para Windows Single-session OS ou Windows Multi-session OS.
2. Extraia o VDA usando as instruções de 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 problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Para obter mais informações, consulte Citrix Insight Services.

Configurar o Universal Print Server

Use as seguintes configurações de política Citrix para configurar o Universal Print Server. Para obter mais informações, consulte a ajuda das configurações de política na tela.

- **Ativar Universal Print Server**. O Universal Print Server está 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 através 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 usada pelo ouvinte CGP (Common Gateway Protocol) do fluxo de dados de impressão do Universal Print Server. O padrão é **7229**.

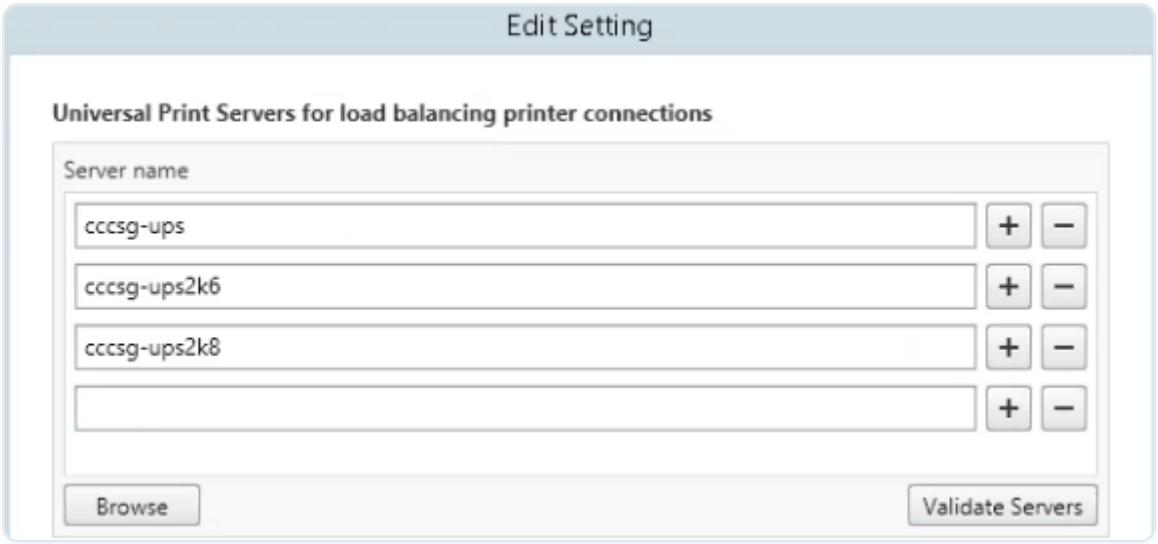
- **Porta do serviço web do Universal Print Server (HTTP/SOAP)**. Especifica o número da porta TCP usada pelo ouvinte do Universal Print Server para solicitações HTTP/SOAP de entrada. O padrão é **8080**.

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 no(s) computador(es) do Universal Print Server:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

Este número de porta deve corresponder à porta do serviço web (HTTP/SOAP) do Universal Print Server da Política HDX, no Studio.

- **Limite de largura de banda de entrada do fluxo de impressão do Universal Print Server (kbps)**. Especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão entregues de cada trabalho de impressão para o Universal Print Server usando CGP. O padrão é 0 (ilimitado).
- **Universal Print Servers para balanceamento de carga**. Esta configuração lista os Universal Print Servers a serem usados para balancear as 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.

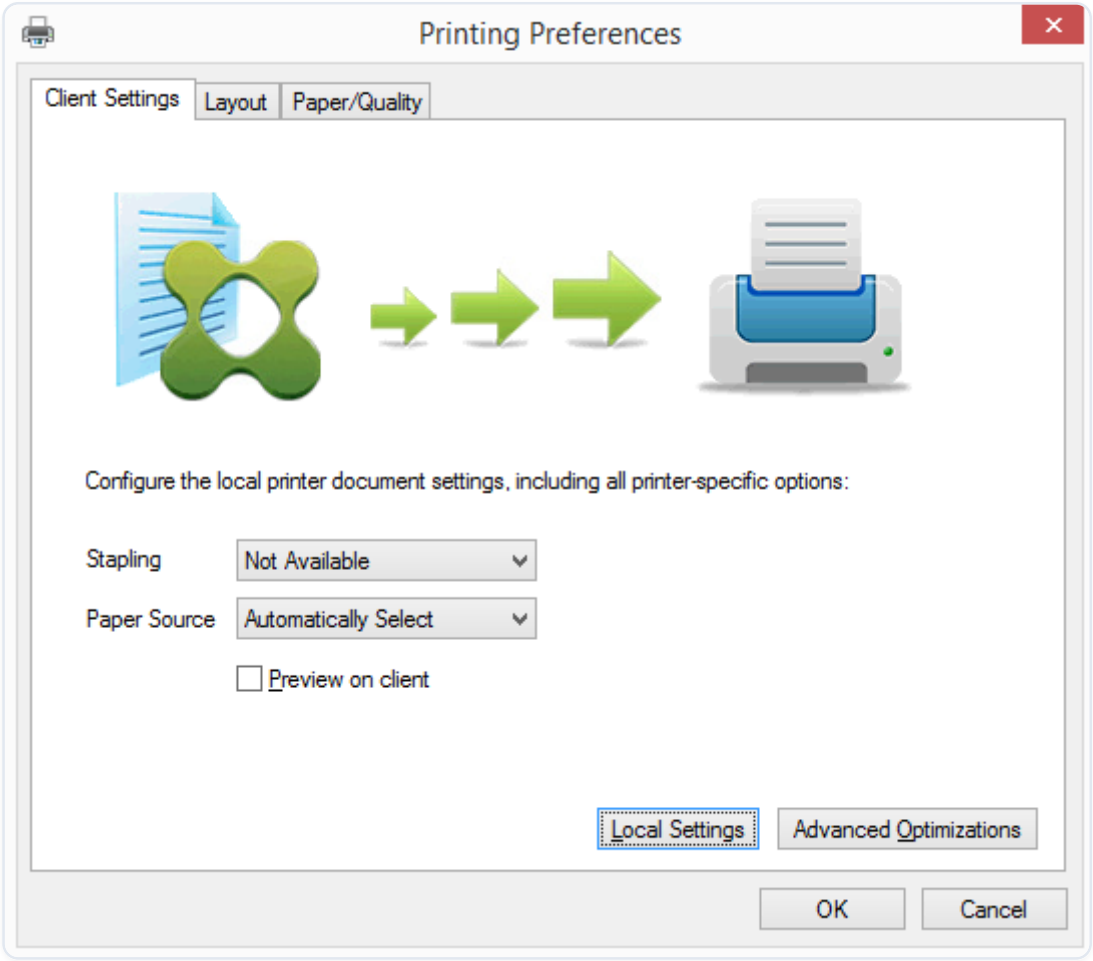
Interações com outras configurações de política - O Universal Print Server respeita outras configurações de política de impressão do Citrix e interage com elas conforme observado na tabela a seguir. As informações fornecidas pressupõem que a configuração de política do Universal Print Server esteja habilitada, os componentes do Universal Print Server estejam instalados e as configurações de política sejam aplicadas.

Configuração da política	**Interação**
Redirecionamento de impressora cliente, Criar automaticamente 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 ao servidor de impressão	Quando o Universal Print Server está habilitado e a configuração da política de uso do driver de impressão universal está configurada para usar apenas a impressão universal, uma conexão direta de impressora de rede pode ser criada com o servidor de impressão, usando o driver de impressão universal.
Preferência de UPD	Suporta drivers EMF e XPS.

Efeitos nas interfaces de usuário - O driver de impressão universal Citrix usado pelo Universal Print Server desabilita os seguintes controles de interface de usuário:

- Na caixa de diálogo Propriedades da Impressora, o botão Configurações da Impressora Local
- Na caixa de diálogo Propriedades do Documento, os botões Configurações da Impressora Local e Visualizar no cliente

O driver de impressão universal Citrix (drivers EMF e XPS) suporta recursos avançados de impressão, como grampeamento e origem do papel. O usuário pode selecionar as opções Grampeamento ou Origem do Papel na caixa de diálogo de impressão UPD personalizada se o cliente ou as impressoras de rede mapeadas para o UPD na sessão suportarem esses recursos.



Para definir configurações de impressora não padrão, como grampeamento e PIN seguro, selecione **Configurações Locais** na caixa de diálogo de impressão UPD do cliente para quaisquer impressoras mapeadas pelo cliente 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 do Esquema de Impressão padronizadas no XML de Capacidades de Impressão. 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 para o Provedor de Impressão Citrix é o mesmo que o Assistente para Adicionar Impressora para o Provedor de Impressão do Windows, com as seguintes exceções:

- Ao adicionar uma impressora por nome ou endereço, você pode fornecer um número de porta HTTP/SOAP para o servidor de impressão. Esse número de porta se torna parte do nome da impressora e aparece nas exibições.
- Se a configuração da política de uso do driver de impressão universal Citrix especificar que a impressão universal deve ser usada, o nome do driver de impressão universal aparecerá ao selecionar uma impressora. O Provedor de Impressão do Windows não pode usar o driver de impressão universal.

O Provedor de Impressão Citrix não oferece suporte à renderização do lado do cliente.

Para obter mais informações sobre o Servidor de Impressão Universal, consulte CTX200328.

Impressoras cliente criadas automaticamente

Estas soluções de impressão universal são fornecidas para impressoras cliente:

- **Impressora Universal Citrix** - Uma impressora genérica criada no início das sessões que não está vinculada a um dispositivo de impressão. A Impressora Universal Citrix não é necessária para enumerar as impressoras cliente disponíveis durante o logon, o que pode reduzir significativamente o uso de recursos e diminuir os tempos de logon do usuário. A Impressora Universal pode imprimir em qualquer dispositivo de impressão do lado do cliente.

  A Impressora Universal Citrix pode não funcionar para todos os dispositivos de usuário ou aplicativos Citrix Workspace™ em seu ambiente. A Impressora Universal Citrix requer um ambiente Windows e não oferece suporte ao Citrix Offline Plug-in ou a aplicativos transmitidos para o cliente. Considere usar impressoras cliente criadas automaticamente e o driver de impressão universal para esses ambientes.

  Para usar uma solução de impressão universal para aplicativos Citrix Workspace que não sejam Windows, use um dos outros drivers de impressão universais baseados em postscript/PCL e instalados automaticamente.
- **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 Citrix genérica 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 os 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 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 seja Permitida (o padrão).

Atribuir impressoras de rede aos usuários

Por padrão, as impressoras de rede no dispositivo do usuário são criadas automaticamente no início das sessões. O sistema permite reduzir o número de impressoras de rede que são enumeradas e mapeadas, especificando as impressoras de rede a serem criadas em cada sessão. Essas impressoras são chamadas de impressoras de sessão.

Você pode filtrar políticas de impressora de sessão por endereço IP para fornecer impressão por proximidade. A impressão por proximidade permite que usuários dentro de um intervalo de endereço IP especificado acessem automaticamente os dispositivos de impressão de rede que existem dentro do mesmo intervalo. A impressão por proximidade é fornecida pelo Citrix Universal Print Server e não requer a configuração descrita nesta seção.

A impressão por proximidade pode envolver o seguinte cenário:

- A rede interna da empresa opera com um servidor DHCP que designa automaticamente endereços IP aos usuários.
- Todos os departamentos da empresa possuem intervalos de endereços IP designados exclusivos.
- As impressoras de rede existem dentro do intervalo de endereços IP de cada departamento.

Quando a impressão por proximidade é configurada e um funcionário se desloca de um departamento para outro, nenhuma configuração adicional do dispositivo de impressão é necessária. Assim que o dispositivo do usuário for reconhecido dentro do intervalo de endereços IP do novo departamento, ele terá acesso a todas as impressoras de rede dentro desse intervalo.

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 em 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 da impressora padrão, selecione uma configuração para Escolher a impressora padrão do cliente:
    - Nome da impressora de rede. As impressoras adicionadas com a configuração de política 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 obter mais informações, consulte a ajuda das configurações de política na tela.
2. Aplique a política ao grupo de usuários (ou outros objetos filtrados) que você deseja afetar.

Configurar impressão por proximidade - A impressão por proximidade também é fornecida pelo Citrix Universal Print Server, que não requer a configuração descrita aqui.

1. Crie uma política separada para cada sub-rede (ou para corresponder ao local da impressora).
2. Em cada política, adicione as impressoras na localização geográfica dessa sub-rede à configuração de Impressoras de sessão.
3. Defina a configuração de 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 Multi-session OS. Além disso, o mapeamento de drivers de impressora permite que você:

- Permitir que impressoras especificadas usem apenas o driver de impressão Citrix Universal
- Permitir ou impedir que impressoras sejam criadas com um driver especificado
- Substituir drivers de impressora bons por drivers desatualizados ou corrompidos
- Substituir um driver disponível no servidor Windows por um nome de driver de cliente

Impedir a instalação automática de drivers de impressora - A instalação automática de drivers de impressão deve ser desabilitada para garantir a consistência entre as máquinas Multi-session OS. Isso pode ser alcançado por meio de políticas Citrix®, políticas Microsoft ou ambas. Para impedir a instalação automática de drivers de impressora nativos do Windows, desabilite a configuração de política Citrix Instalação automática de drivers de impressora internos.

Mapear drivers de impressora cliente - Cada cliente fornece informações sobre as 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 de cliente redirecionadas.

Aqui está o processo geral para definir regras de substituição de driver e editar configurações de impressão para drivers de impressora cliente mapeados:

1. Para especificar regras de substituição de driver para impressoras cliente criadas automaticamente, configure a configuração de política Citrix Printer driver mapping and compatibility 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 Find printer driver. 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 Do not create.
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 Settings 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. Esta 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 o mapeamento dos drivers, pois algumas funcionalidades da impressora podem estar disponíveis apenas com um driver específico.

Quando os usuários fazem logon, o sistema verifica a lista de compatibilidade do driver da impressora cliente antes de configurar as impressoras cliente.

Otimizar o desempenho da impressão

To optimize printing performance, use the Universal Print Server and Universal print driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults. Specifies default settings for the Universal Printer when it is created for a session:
    - A qualidade de imagem desejada especifica o limite de compressão de imagem padrão aplicado à impressão universal. Por padrão, a Standard Quality está ativada, o que significa que os usuários só podem imprimir imagens usando compressão de qualidade padrão ou reduzida.
    - Ativar compressão pesada habilita ou desabilita a redução da largura de banda além do nível de compressão definido pela qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compressão pesada está desabilitada.

    - As configurações de Cache de Imagem e Fonte especificam se as imagens e fontes que aparecem várias vezes no fluxo de impressão devem ou não ser armazenadas em cache, garantindo que cada imagem ou fonte única 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 compressão de imagem de impressão universal. Define a qualidade máxima e o nível mínimo de compressão disponíveis para imagens impressas com o driver de impressão universal. Por padrão, o limite de compressão de imagem é definido como Melhor Qualidade (compressão sem perdas).
- Limite de qualidade de impressão universal. Especifica o máximo de pontos por polegada (dpi) disponível para gerar saída impressa na sessão. Por padrão, nenhum limite é especificado.

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina do SO de múltiplas sessões, através da rede e diretamente para o servidor de impressão. Considere rotear trabalhos de impressão pela conexão ICA® se a rede tiver latência substancial ou largura de banda limitada. Para fazer isso, desative a configuração da política Citrix Conexões diretas a servidores de impressão. Os dados enviados pela conexão ICA são compactados, de modo que menos largura de banda é consumida à medida que os dados viajam pela WAN.

Melhore o desempenho da sessão limitando a largura de banda de impressão - Ao imprimir arquivos de máquinas do SO de múltiplas sessões para impressoras de usuário, outros canais virtuais (como vídeo) podem ter desempenho reduzido devido à competição por largura de banda, especialmente se os usuários acessarem servidores por meio de redes mais lentas. Para evitar essa degradação, você pode limitar a largura de banda usada pela impressão do usuário. Ao limitar a taxa de transmissão de dados para impressão, você disponibiliza mais largura de banda no fluxo de dados HDX™ para transmissão de vídeo, 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 largura de banda da impressora da política Citrix para configurar os limites de largura de banda da sessão de impressão. Para definir os limites para o site, execute esta tarefa usando o Studio. Para definir os limites para servidores individuais, execute esta tarefa usando o Console de Gerenciamento de Política de Grupo no Windows localmente em cada máquina do SO de múltiplas sessões.

- A configuração Limite de largura de banda de redirecionamento de impressora especifica a largura de banda disponível para impressão em kilobits por segundo (kbps).
- A configuração Porcentagem do limite de largura de banda de redirecionamento de impressora limita a largura de banda disponível para impressão a uma porcentagem da largura de banda geral disponível.

  Nota: Para especificar a largura de banda como uma porcentagem usando a configuração Porcentagem do limite de largura de banda de redirecionamento de impressora, ative 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 servidores de impressão universais fora de serviço, para distribuir a carga de impressão por 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 de entrada funcionem normalmente sem afetar a experiência do usuário e sem exigir intervenção imediata do administrador.

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 Microsoft Management Console; UAC Desativado: Pré-Windows 8: Painel de Controle, Windows 8: Snap-in de Gerenciamento de Impressão

	CAMINHO DE IMPRESSÃO	LOCALIZAÇÃO
Impressoras de servidor de rede local (Impressoras de um servidor de impressão de rede que são adicionadas a uma máquina de SO multi-sessão)	Caminho de impressão de rede	UAC Ativado: Servidor de Impressão \> Painel de Controle; UAC Desativado: Servidor de Impressão \> Painel de Controle

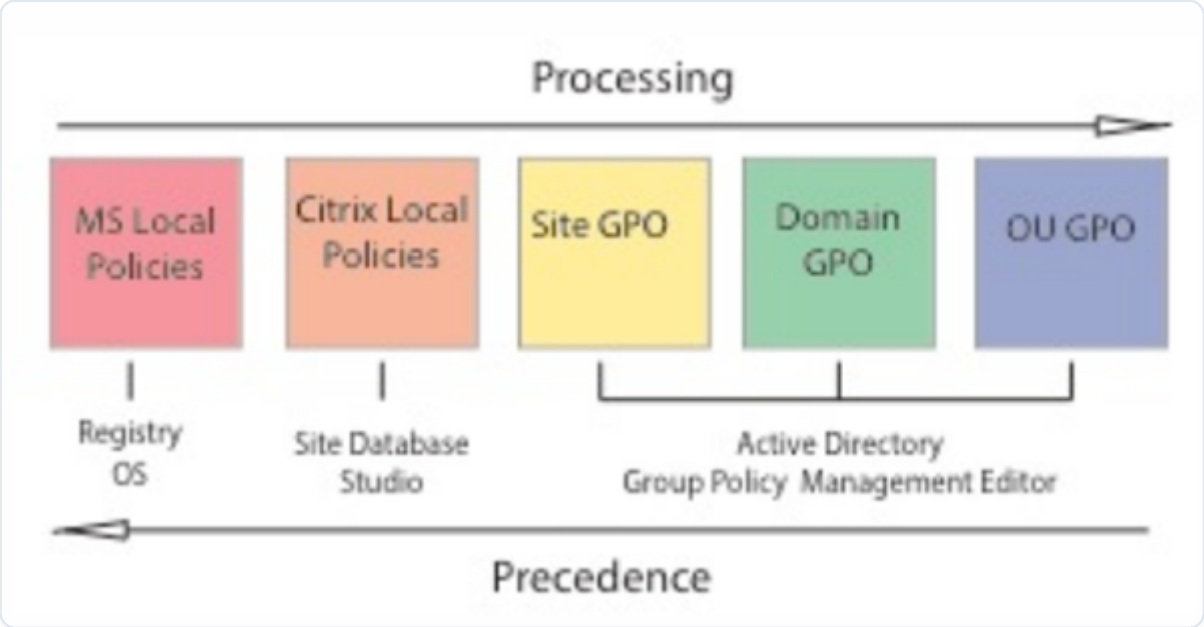
Nota:

As filas de impressão para impressoras de rede que usam o caminho de impressão de rede são privadas e não podem ser gerenciadas através do sistema.

Políticas

Políticas são uma coleção de configurações que definem como sessões, largura de banda e segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.

Você pode aplicar configurações de política a máquinas físicas e virtuais ou a usuários. Você pode aplicar configurações a usuários individuais no nível local ou em grupos de segurança em um Active Directory. As configurações definem critérios e regras específicos. Se você não atribuir as políticas especificamente, as configurações serão aplicadas a todas as conexões.



Você pode aplicar políticas em diferentes níveis da rede. As configurações de política colocadas no nível GPO da Unidade Organizacional têm a precedência mais alta na rede. As políticas no nível GPO do Domínio substituem as políticas no nível do Objeto de Política de Grupo do Site. O nível do Objeto de Política de Grupo do Site substitui quaisquer políticas conflitantes nos níveis de Políticas Locais da Microsoft e da Citrix.

Todas as Políticas Locais da Citrix são criadas e gerenciadas no console do Citrix 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 ao 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

Configure as políticas Citrix® para controlar o acesso do usuário e os ambientes de sessão. As políticas Citrix são o método mais eficiente de controlar as configurações de conexão, segurança e largura de banda. Você pode criar políticas para grupos específicos de usuários, dispositivos ou tipos de conexão. Cada política pode conter várias configurações.

Ferramentas para trabalhar com políticas Citrix

Você pode usar as seguintes ferramentas com as políticas Citrix.

- **Studio** - Se você for um administrador Citrix sem permissão para gerenciar a política de grupo, use o Studio para criar políticas para seu site. As políticas criadas usando o Studio são armazenadas no banco de dados do site. E as atualizações são enviadas para a área de trabalho virtual quando essa área de trabalho virtual se registra no broker ou quando um usuário se conecta a essa área de trabalho virtual.
- **Editor de Política de Grupo Local** (snap-in do Microsoft Management Console) - Se 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:**
>
> Use o Editor de Política de Grupo Local para configurar algumas configurações de política. Essas configurações de política incluem aquelas relacionadas ao registro de VDAs com um controlador. Além disso, aquelas configurações relacionadas a servidores Microsoft App-V.

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 XenApp ou XenDesktop® (armazenado no banco de dados do Site)
3. GPOs no nível do 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. Essa configuração significa que as configurações de política têm precedência na seguinte ordem:

1. Unidades Organizacionais
2. GPOs de nível de domínio
3. GPOs no nível do Site
4. GPO do Site XenApp® ou XenDesktop (armazenado no banco de dados do Site)
5. GPO Local

Por exemplo, um administrador Citrix usa o 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. A razão é que a Política B foi processada no nível do domínio e a Política A foi processada no nível do GPO do Site XenApp ou XenDesktop.

No entanto, quando um usuário inicia uma sessão ICA® ou de Protocolo de Área de Trabalho Remota (RDP), 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 visualização do conteúdo da janela ao arrastar.

Ao usar várias políticas, você pode priorizar políticas que contêm configurações conflitantes. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

Fluxo de trabalho para políticas Citrix

O processo para configurar políticas é o seguinte:

1. Crie a política.
2. Configure as configurações da política.

3. Atribua a política a objetos de máquina e usuário.
4. Priorize a política.
5. Verifique a política efetiva executando o assistente de Modelagem de Política de Grupo Citrix.

> **Nota:**
>
> Você abre o assistente de Modelagem de Política de Grupo Citrix navegando até a guia **Políticas > Modelagem** e, em seguida, clicando em **Iniciar Assistente de Modelagem** no painel **Ações**. A guia **Modelagem** não está disponível no Studio hospedado no Citrix Cloud.

navegar políticas e configurações Citrix

No Editor de Política de Grupo Local, as políticas e configurações aparecem em duas categorias: Configuração do Computador e Configuração do Usuário. Cada categoria tem um nó de Políticas Citrix. Consulte a documentação da Microsoft para obter detalhes sobre como navegar e usar este snap-in.

No 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.

- Configurações de computador (configurações de política aplicadas a máquinas) definem o comportamento de 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 de navegação do Studio.

  - A guia **Políticas** lista todas as políticas. Ao selecionar uma política, as guias à direita exibem:
    - Visão geral (nome, prioridade, status ativado/desativado e descrição)
    - Configurações (lista de configurações configuradas)

    - Atribuído a (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 à direita 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.
  - Na guia **Modelagem**, você pode simular cenários de conexão com políticas Citrix. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

    > **Nota:**
    >
    > A guia **Modelagem** não está disponível no Studio hospedado no Citrix Cloud.

  Para pesquisar uma configuração em uma política ou modelo:

  a. Selecione a política ou o modelo.
  b. Selecione **Editar política** ou **Editar modelo** no painel **Ações**.
  c. Na página Configurações, comece a digitar o nome da configuração.

  Você pode refinar sua pesquisa selecionando:

  - Uma versão específica do produto
  - Uma categoria (por exemplo, Largura de banda)
  - 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.

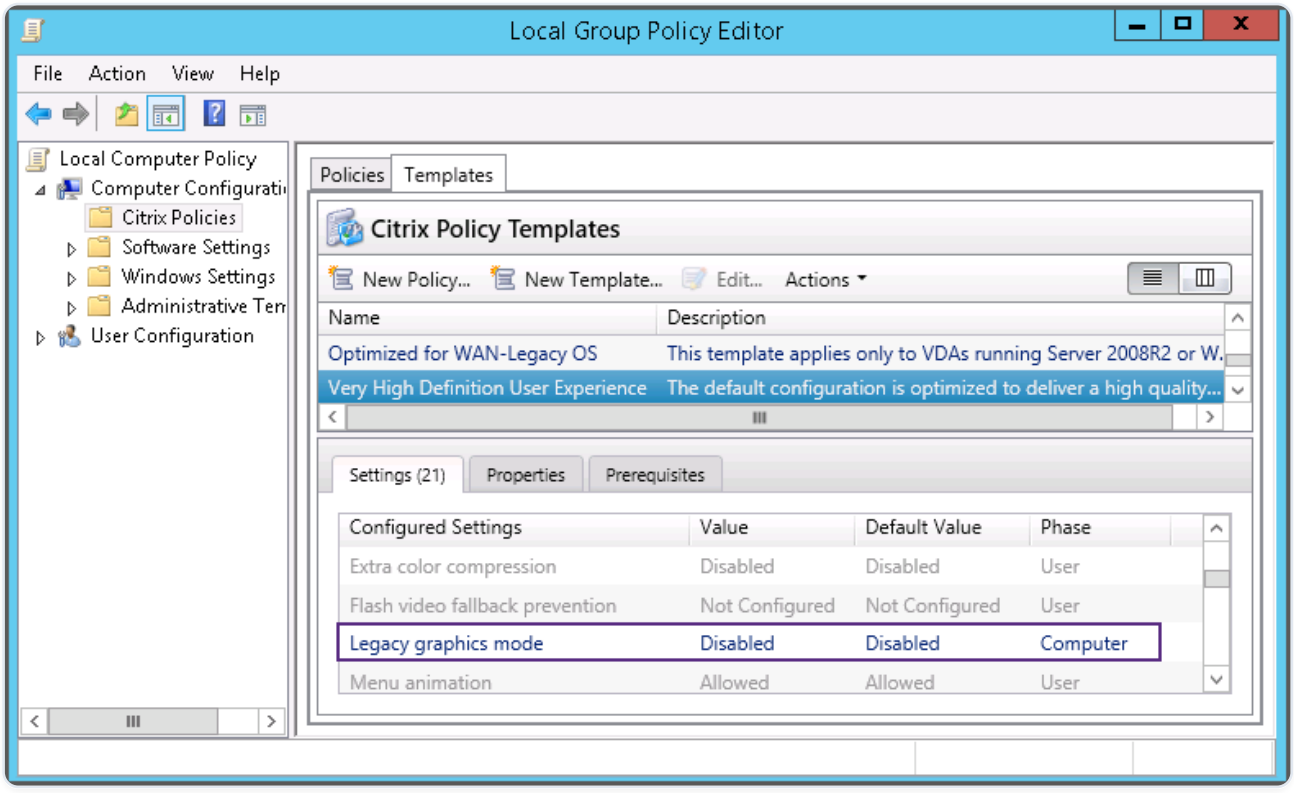
Você pode refinar sua pesquisa selecionando uma versão específica do produto ou selecionando uma categoria. Para uma pesquisa não filtrada, selecione **Todas as Configurações**.

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 Studio, políticas e modelos são exibidos em uma única lista, independentemente de conterem configurações de usuário, computador ou ambos os tipos. Além disso, políticas e modelos podem ser aplicados usando filtros de usuário e de computador.

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 Definição Muito Alta 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

Modelos são uma fonte para criar políticas a partir de um ponto de partida predefinido. Os modelos Citrix® integrados, otimizados para ambientes específicos ou condições de rede, podem ser usados como:

- Uma fonte para criar suas próprias políticas e modelos para compartilhar entre sites.
- Uma referência para facilitar a comparação de resultados entre implantações, pois você pode citar os resultados, por exemplo, "...ao usar o modelo Citrix x ou y...".
- Um método para comunicar políticas com o Suporte Citrix ou terceiros confiáveis importando ou exportando modelos.

Os modelos de política podem ser importados e exportados.

Para considerações ao usar modelos para criar políticas, consulte o artigo do Knowledge Center CTX202330. Para baixar o PDF, faça login usando suas credenciais.

Modelos Citrix integrados

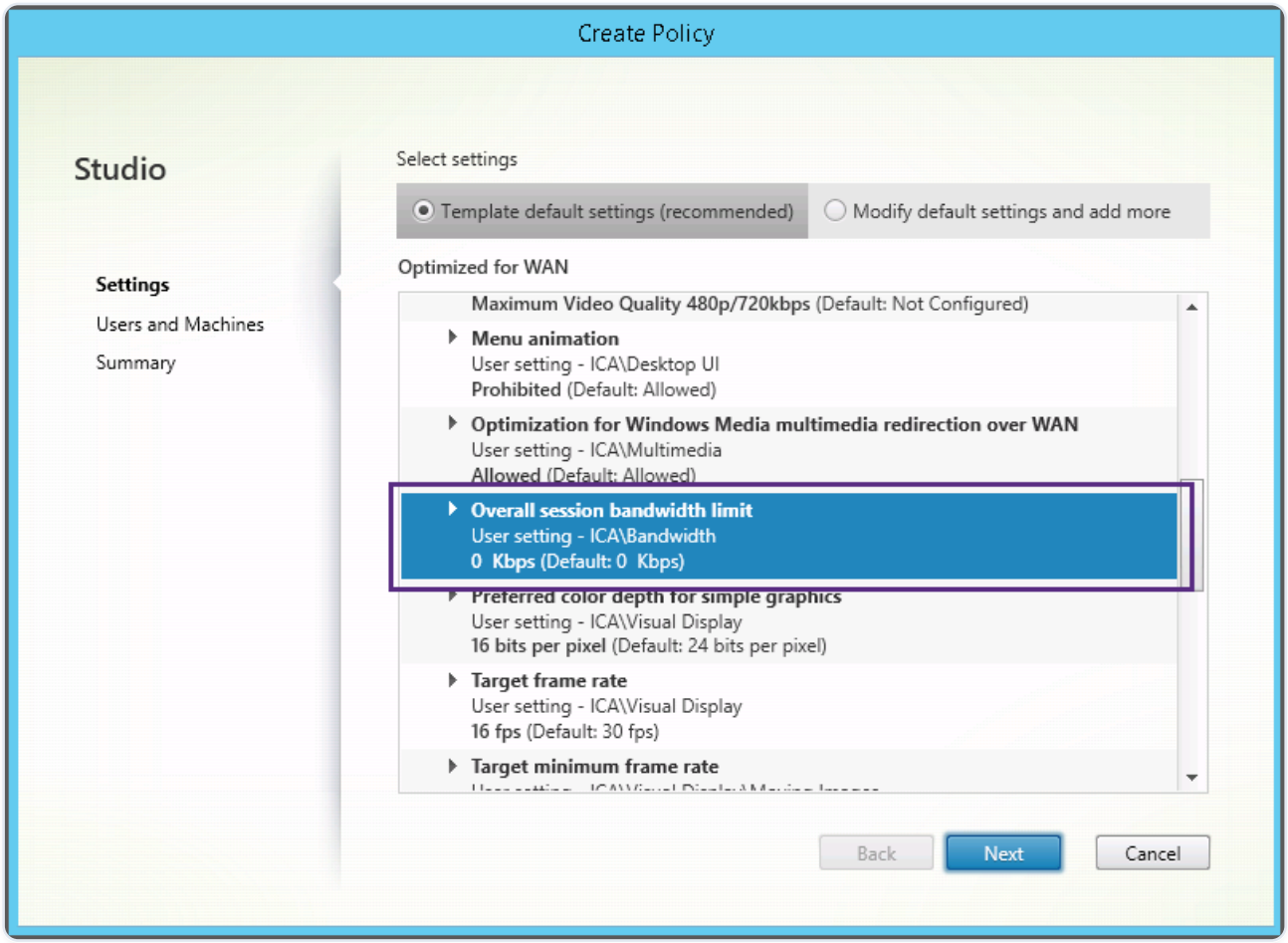
Os seguintes modelos de política estão disponíveis:

- **Experiência do Usuário de Definição Muito Alta**. Este modelo impõe configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde várias 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 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.
- **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* se aplica 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 a impressão, área de transferência, dispositivos periféricos, mapeamento de unidade, redirecionamento de porta e aceleração Flash em dispositivos de usuário. A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade de usuários por servidor.

Embora recomendemos o uso dos modelos Citrix integrados com suas configurações padrão, existem configurações que não possuem um valor recomendado específico. Por exemplo, **Overall session bandwidth limit**, 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 de Alta Escalabilidade de Servidor e Otimizado para WAN, use as versões de SO herdadas 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 Studio

Para criar um modelo com base em um modelo:

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Modelos** e, em seguida, selecione o modelo a partir do qual você criará o modelo.
3. Selecione **Criar Modelo** no painel Ações.
4. Selecione e configure as configurações de política a serem incluídas no modelo. Remova quaisquer configurações existentes que não pertençam. Insira um nome para o modelo.

Depois de clicar em **Concluir**, o novo modelo aparece na guia **Modelos**.

Para criar um modelo com base em uma política:

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Políticas** e, em seguida, selecione a política a partir da qual você criará o modelo.
3. Selecione **Salvar como Modelo** no painel Ações.
4. Selecione e configure quaisquer novas configurações de política para incluir no modelo. Remova quaisquer configurações existentes que não pertençam. Insira um nome e uma descrição para o modelo e, em seguida, clique em **Concluir**.

Para importar um modelo:

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Modelos** e, em seguida, selecione **Importar Modelo**.

3. Selecione o arquivo de modelo a ser importado e, em seguida, clique em **Abrir**. Se você importar um modelo com o mesmo nome de um modelo existente, poderá optar por sobrescrever o modelo existente ou salvar o modelo com um nome diferente que é gerado automaticamente.

Para exportar um modelo:

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Modelos** e, em seguida, selecione **Exportar Modelo**.
3. Selecione o local onde deseja salvar o modelo e, em seguida, clique em **Salvar**.

Um arquivo `.gpt` é criado no local especificado.

Criar e gerenciar modelos 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 um modelo a partir de uma política existente	Na guia **Políticas**, selecione a política e, em seguida, selecione **Ações > Salvar como Modelo**.
Criar uma política a partir de um modelo existente	Na guia **Modelos**, selecione o modelo e, em seguida, clique em **Nova Política**.
Criar um modelo a partir de um modelo existente	Na guia **Modelos**, selecione o modelo e, em seguida, clique em **Novo Modelo**.
Importar um modelo	Na guia **Modelos**, selecione **Ações > Importar**.
Exportar um modelo	Na guia **Modelos**, selecione **Ações > Exportar**.
Exibir configurações do modelo	Na guia **Modelos**, selecione o modelo e, em seguida, clique na guia **Configurações**.
Exibir um resumo das propriedades do modelo	Na guia **Modelos**, selecione o modelo e, em seguida, clique na guia **Propriedades**.

TAREFA	INSTRUÇÃO
Exibir pré-requisitos do modelo	Na guia **Modelos**, selecione o modelo e, em seguida, clique na guia **Pré-requisitos**.

Modelos e administração delegada

Os modelos de política são armazenados na máquina onde o pacote de gerenciamento de políticas foi instalado. Esta máquina é a máquina do Delivery Controller ou a máquina de gerenciamento de Objetos de Política de Grupo — não o banco de dados do Site do Citrix Virtual Apps and Desktops. Isso significa que as permissões administrativas do Windows controlam os arquivos de modelo de política, em vez das funções e escopos de administração delegada do site.

Como resultado, um administrador com permissão somente leitura no Site pode, por exemplo, criar modelos. No entanto, como os modelos são arquivos locais, nenhuma alteração é feita no seu ambiente.

Os modelos personalizados são visíveis apenas para a conta de usuário que os cria e são armazenados no perfil do Windows do usuário. Para expor um modelo personalizado ainda mais, crie uma política a partir dele ou exporte-o para um local compartilhado.

Criar políticas

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. Depois de editar a política, configure as configurações apropriadas. Evite criar uma política apenas para habilitar uma configuração específica ou para excluir a política de se aplicar a determinados usuários.

Ao criar uma política, você pode baseá-la 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 Citrix Studio, as novas políticas criadas são definidas como Desabilitadas, a menos que a caixa de seleção **Habilitar política** seja explicitamente marcada.

Configurações de política

As configurações de política podem ser habilitadas, desabilitadas ou não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

Algumas configurações de política podem estar em um dos seguintes estados:

- Permitido ou Proibido permite ou impede a ação controlada pela configuração. Às vezes, os usuários são permitidos ou impedidos de gerenciar a ação da configuração em uma sessão. Por exemplo, se a configuração de animação de menu for definida como Permitido, os usuários poderão controlar as animações de menu em seu ambiente cliente.
- Habilitado ou Desabilitado liga ou desliga 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 cliente controla se os usuários têm permissão para acessar as unidades em seus dispositivos. Tanto esta configuração quanto a configuração **Unidades de rede cliente** devem ser adicionadas à política para permitir que os usuários acessem suas unidades de rede. Se a configuração **Redirecionamento de unidade cliente** estiver desabilitada, os usuários não poderão acessar suas unidades de rede, mesmo que a configuração **Unidades de rede 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 fizerem logon. Se você estiver usando o Active Directory, as configurações de política serão atualizadas quando o Active Directory reavaliar as políticas em intervalos de 90 minutos. E as configurações de política são aplicadas quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon.

Para algumas configurações de política, você pode inserir ou selecionar um valor ao adicionar a configuração a uma política. Você pode limitar a configuração da configuração selecionando Usar valor padrão. Essa seleção desabilita a configuração da configuração e permite que apenas o valor padrão da configuração seja usado quando a política for aplicada. Essa seleção é independente do valor que foi inserido antes de selecionar Usar valor padrão.

Como melhor prática:

- 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.
- Desabilite políticas não utilizadas. Políticas sem configurações adicionadas criam processamento desnecessário.

Atribuições de diretiva

Ao criar uma diretiva, você a atribui a determinados usuários e objetos de máquina. Essa diretiva é aplicada às conexões de acordo com critérios ou regras específicos. Em geral, você pode adicionar quantas atribuições quiser a uma diretiva, com base em uma combinação de critérios. Se você não especificar nenhuma atribuição, a diretiva será aplicada a todas as conexões.

A tabela a seguir lista as atribuições disponíveis:

NOME DA ATRIBUIÇÃO	APLICA UMA DIRETIVA COM BASE EM
Controle de Acesso	Condições de controle de acesso através das quais um cliente está se conectando. *Tipo de conexão* - Se a diretiva deve ser aplicada a conexões feitas com ou sem o NetScaler® Gateway. *Nome do farm do NetScaler Gateway* - Nome do servidor virtual do NetScaler Gateway. *Condição de acesso* - Nome da diretiva de análise de ponto de extremidade ou diretiva 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 diretiva.
Endereço IP do Cliente	Endereço IP do dispositivo do usuário usado para se conectar à sessão: Exemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70,

NOME DA ATRIBUIÇÃO	APLICA UMA DIRETIVA COM BASE EM
	12.0.0.1/24; Exemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nome do Cliente	Nome do dispositivo do usuário. Correspondência exata: ClientABCName. Usando curinga: Client*Name.
Grupo de Entrega	Associação ao Grupo de Entrega.
Tipo de Grupo de Entrega	Tipo de área de trabalho ou aplicativo: área de trabalho privada, área de trabalho compartilhada, aplicativo privado ou aplicativo compartilhado. **Nota:** As opções de filtro de área de trabalho privada e área de trabalho compartilhada estão disponíveis apenas para Citrix Virtual Apps and Desktops 7.x. Para obter mais informações, consulte CTX219153.
Unidade Organizacional (OU)	Unidade organizacional.
Tag	Tags. **Nota:** Aplique esta política a todas as máquinas marcadas com tags. 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 estão configuradas são ignoradas.

Importante:

Ao configurar políticas do Active Directory e do Citrix usando o Console de Gerenciamento de Política de Grupo, as atribuições e configurações podem não ser aplicadas conforme o esperado. Para obter mais informações, consulte CTX127461

> Uma política chamada "Unfiltered" é fornecida por padrão.

- Se você usar o Studio para gerenciar políticas Citrix, as configurações que você adicionar à política Não Filtrada são aplicadas a todos os servidores, desktops e conexões em um Site.
- Se você usar o Editor de Política de Grupo Local para gerenciar políticas Citrix, as configurações que você adicionar à política Não Filtrada são 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 OU de Vendas inclui um GPO chamado Vendas-EUA que inclui todos os membros da equipe de vendas dos EUA. O GPO Vendas-EUA é configurado com uma política Não Filtrada que inclui várias configurações de política de usuário. Quando o gerente de Vendas dos EUA faz logon no Site, as configurações da política Não Filtrada são aplicadas automaticamente à sessão. Essa configuração ocorre porque o usuário é membro do GPO Vendas-EUA.

O modo de uma atribuição determina se a política é aplicada apenas a conexões que correspondem a todos os critérios de atribuição. Se o modo for definido como Permitir (o padrão), a política será aplicada apenas a conexões que correspondem aos critérios de atribuição. Se o modo for definido como Negar, a política será aplicada se a conexão não corresponder aos critérios de atribuição. Os exemplos a seguir ilustram como os modos de atribuição afetam as políticas Citrix quando várias atribuições estão presentes.

- **Exemplo: Atribuições do mesmo tipo com modos diferentes** - Em políticas com duas atribuições do mesmo tipo, uma definida como Permitir e outra como Negar, a atribuição definida como Negar tem precedência, desde que a conexão satisfaça ambas as atribuições. Por exemplo:

  A Política 1 inclui as seguintes atribuições:

  - A Atribuição A especifica o grupo 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 está definido como Permitir.
- A Atribuição D é uma atribuição de Endereço IP do Cliente que especifica 10.8.169.* (a rede corporativa). O modo está definido como Permitir.

Quando o gerente de Vendas faz logon no Site do escritório, a política é aplicada porque a conexão satisfaz ambas as atribuições.

A Política 3 inclui as seguintes atribuições:

- A Atribuição E é uma atribuição de Usuário que especifica o grupo de Vendas. O modo está definido como Permitir.
- A Atribuição F é uma atribuição de Controle de Acesso que especifica as condições de conexão do NetScaler Gateway. O modo está definido como Permitir.

Quando o gerente de vendas faz logon no Site do escritório, a política não é aplicada porque a conexão não satisfaz a Atribuição F.

Criar uma política com base em um modelo, usando o Studio

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Modelos** e selecione um modelo.
3. Selecione **Criar Política** a partir de **Modelo** no painel **Ações**.
4. Por padrão, a nova política usa todas as configurações padrão do modelo. Neste caso, a opção **Usar configurações padrão do modelo** está selecionada. Se você quiser alterar as configurações, selecione **Modificar padrões e adicionar mais configurações** e, em seguida, adicione ou remova configurações.
5. Especifique como aplicar a política selecionando 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 nome padrão. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

   A política é habilitada por padrão; você pode desativá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem logon. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

Criar uma política usando o Studio

1. Selecione **Políticas** no painel de navegação do Studio.
2. Selecione a guia **Políticas**.
3. Selecione **Criar Política** no painel **Ações**.
4. Adicione e configure as configurações da política.
5. Especifique como aplicar a política escolhendo uma das seguintes opções:

   - Atribua a objetos de usuário e máquina selecionados e, em seguida, selecione os objetos de usuário e máquina aos quais a política deve ser aplicada.
   - Atribua a todos os objetos em um site para aplicar a política a todos os objetos de usuário e máquina no Site.

6. Insira um nome para a política ou aceite o padrão. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

   A política é habilitada por padrão; você pode desativá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem logon. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

Criar e gerenciar políticas usando o Editor de Política de Grupo

No Editor de Política de Grupo, expanda **Configuração do Computador ou Configuração do Usuário**. Expanda o nó **Políticas** e selecione **Políticas Citrix**. Escolha a ação apropriada:

TAREFA	INSTRUÇÃO
Criar uma política	Na guia **Políticas**, clique em **Novo**.

TAREFA	INSTRUÇÃO
Editar uma política existente	Na guia **Políticas**, selecione a política e clique em **Editar**.
Alterar a prioridade de uma política existente	Na guia **Políticas**, selecione a política e clique em **Superior** ou **Inferior**.
Exibir informações de resumo sobre uma política	Na guia **Políticas**, selecione a política e clique na guia **Resumo**.
Exibir e alterar as configurações da política	Na guia **Políticas**, selecione a política e clique na guia **Configurações**.
Exibir e alterar os filtros da 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 então selecione **Ações > Habilitar** ou **Ações > Desabilitar**.
Criar uma política a partir de um modelo existente	Na guia **Modelos**, selecione o modelo e então clique em **Nova Política**.

Comparar, priorizar, modelar e solucionar problemas de políticas

Você pode usar várias políticas para personalizar seu ambiente e atender às necessidades dos usuários com base em suas funções de trabalho, localizações geográficas ou tipos de conexão. Por exemplo, para segurança aprimorada, imponha restrições a grupos de usuários que interagem regularmente com dados confidenciais.

Você também pode criar uma política que 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 pode criar outra política apenas para esses usuários. Em seguida, você classifica ou prioriza as duas políticas para controlar qual delas tem precedência. Ao usar várias políticas, você deve determinar:

- Como priorizar as políticas

- Como criar exceções
- Como visualizar a política efetiva quando as políticas entram em conflito.

Em geral, as políticas substituem configurações semelhantes configuradas para todo o Site, para Delivery Controllers específicos ou no dispositivo do usuário. A exceção a este princípio é a segurança. A configuração de criptografia mais alta em seu ambiente sempre substitui outras configurações e políticas. A configuração de criptografia mais alta inclui o sistema operacional e as configurações de sombreamento mais restritivas.

As políticas Citrix® interagem com as políticas que você define em seu sistema operacional. Em um ambiente Citrix, as configurações Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou usando a Configuração do Host da Sessão da Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão de cliente do Protocolo de Área de Trabalho Remota (RDP). As configurações típicas de RDP incluem configurações como papel de parede da área de trabalho, animação de menu e visualização do conteúdo da janela ao arrastar.

Algumas configurações de política, como Secure ICA®, devem corresponder às configurações do sistema operacional. Se um nível de criptografia de prioridade mais alta for definido em outro lugar, as configurações da **política Secure ICA** que você especificar na política ou ao entregar aplicativos e desktops poderão ser substituídas.

Por exemplo, as configurações de criptografia que você especifica ao criar Grupos de Entrega devem estar no mesmo nível das configurações de criptografia que você especificou em todo o seu ambiente.

> **Observação:**
>
> No segundo salto de cenários de salto duplo, considere que um VDA de SO de sessão única se conecta a um VDA de SO de múltiplas sessões. Neste caso, as políticas Citrix atuam no VDA de SO de sessão única como se fosse o dispositivo do usuário. Por exemplo, considere que as políticas estão configuradas para armazenar imagens em cache no dispositivo do usuário. Neste exemplo, as imagens armazenadas em cache para o segundo salto em um cenário de salto duplo são armazenadas em cache na máquina VDA de SO de sessão única.

Comparar políticas e modelos

Você pode comparar as configurações em uma política ou modelo com as configurações das outras políticas ou modelos. Por exemplo, você pode precisar verificar os valores das configurações para manter a conformidade com as melhores práticas. Você também pode querer comparar as configurações em uma política ou modelo com as configurações padrão fornecidas pela Citrix.

1. Selecione Políticas no painel de navegação do Studio.
2. Clique na guia Comparação e, em seguida, clique em Selecionar.
3. Escolha as políticas ou modelos para comparar. 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

Priorizar políticas permite definir a precedência das políticas quando elas contêm configurações conflitantes. Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas em ordem de prioridade e várias instâncias de qualquer configuração são comparadas. Cada configuração é aplicada de acordo com a classificação de prioridade da política.

Você prioriza políticas atribuindo-lhes diferentes números de prioridade no Studio. Por padrão, as novas políticas recebem a prioridade mais baixa. Se as configurações de política entrarem em conflito, uma política com prioridade mais alta (um número de prioridade 1 é o mais alto) substitui uma política com prioridade mais baixa. As configurações são mescladas de acordo com a prioridade e a condição da configuração. Por exemplo, se a configuração está desabilitada ou habilitada. Qualquer configuração desabilitada substitui uma configuração de classificação inferior que esteja habilitada. As configurações de política que não estão configuradas são ignoradas e não substituem as configurações de classificações inferiores.

1. Selecione **Políticas** no painel de navegação do Studio. Certifique-se de que a guia **Políticas** esteja selecionada.
2. Selecione uma política.
3. Selecione **Prioridade Inferior** ou **Prioridade Superior** no painel **Ações**.

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 mais alto do que a política para todo o grupo
- 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

Às vezes, uma conexão não responde como esperado porque várias políticas se aplicam. Se uma política de prioridade mais alta se aplicar a uma conexão, ela poderá substituir as configurações que você configura 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 do Citrix que provavelmente entrariam em vigor no

cenário. Considere que você está conectado ao Controller como um usuário de domínio. Neste caso, o assistente calcula o Conjunto Resultante de Política usando as configurações de política do site e os Objetos de Política de Grupo (GPOs) do Active Directory.

- Use os Resultados da Política de Grupo para produzir um relatório descrevendo as políticas do 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 do Citrix, estão sendo aplicados atualmente a um usuário e controlador específicos.

Você pode iniciar o Assistente de Modelagem de Política de Grupo do Citrix no painel **Ações** no **Citrix Studio**. Você pode iniciar qualquer uma das ferramentas no Console de Gerenciamento de Política de Grupo no Windows.

As configurações de política do site criadas usando o Studio não são incluídas no Conjunto Resultante de Política nos seguintes casos:

- Se você executar o Assistente de Modelagem de Política de Grupo do Citrix a partir do Console de Gerenciamento de Política de Grupo Ou,
- 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 Studio, a menos que você crie políticas usando apenas o Console de Gerenciamento de Política de Grupo.

Use o Assistente de Modelagem de Política de Grupo do Citrix

Abra o Assistente de Modelagem de Política de Grupo do Citrix usando uma das seguintes opções:

- Selecione Políticas no painel de navegação do Studio, selecione a guia Modelagem e, em seguida, selecione Iniciar Assistente de Modelagem no painel Ações.
- Inicie o Console de Gerenciamento de Política de Grupo (gpmc.msc), clique com o botão direito do mouse em Modelagem de Política de Grupo do Citrix no painel de árvore e, em seguida, selecione Assistente de Modelagem de Política de Grupo do Citrix.

Siga as instruções do assistente para selecionar o seguinte:

- Controlador de domínio

- Usuários
- Computadores
- Configurações de ambiente
- Critérios de atribuição do Citrix a serem usados na simulação.

Depois de clicar em **Concluir**, o assistente gera um relatório dos resultados da modelagem. No Studio, o relatório aparece no painel central, na guia **Modelagem**.

Para visualizar o relatório, selecione **Exibir Relatório de Modelagem**.

> **Observação:**
>
> A guia **Modelagem** não está disponível no Studio hospedado no Citrix Cloud.

Solucionar problemas de políticas

Usuários, endereços IP e outros objetos atribuídos podem ter várias políticas aplicadas simultaneamente. Esse cenário pode resultar em conflitos em que uma política pode não se comportar como esperado. Ao executar o Assistente de Modelagem de Política de Grupo do 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. Essa situação ocorre quando:

- Nenhuma política tem atribuições que correspondam aos critérios de avaliação da política.
- Políticas que correspondem à atribuição não têm nenhuma configuração definida.
- 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 tenham 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 multiusuário 7 até o atual
Número da porta do listener ICA	1494	Todas as versões de VDA
Inicialização de programas não publicados durante a conexão do cliente	Proibido	VDA para SO multi-sessão 7 até o atual
Limitar o tamanho da transferência da área de transferência do cliente para a sessão	Desabilitado	VDA 2009
Limitar o tamanho da transferência da área de transferência da sessão para o cliente	Desabilitado	VDA 2009
Modo tolerante a perdas	Permitido	VDA 2003. Nota: O modo de tolerância a perdas ainda não está disponível. Esta versão do VDA o suporta quando ele se tornar disponível.
Limites de tolerância a perdas	Quando o modo tolerante a perdas estiver disponível: Perda de pacote: 5%, Latência: 300 ms (RTT)	VDA 2003 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
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
Formatos permitidos para gravação da área de transferência da sessão	Nenhum formato é 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 configuração usando o registro.
Lista de permissões de canal virtual	Ativado	VDA 2109

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 várias sessões de VDAs usando Citrix Virtual Apps

NOME	CONFIGURAÇÃO PADRÃO	VDA
		and Desktops™ 2109 ou posterior.
Áudio sobre transporte em tempo real UDP	Permitido	Todas as versões de VDA
Plug N Play de áudio	Permitido	VDA para SO de várias sessões 7 até o atual
Qualidade do áudio	Alta - áudio de alta definição	Todas as versões de VDA
Redirecionamento de áudio do cliente	Permitido	Todas as versões de VDA
Redirecionamento de microfone do cliente	Permitido	Todas as versões de VDA

ICA/Reconexão automática do cliente

NOME	CONFIGURAÇÃO PADRÃO	VDA
Reconexão automática do cliente	Permitido	Todas as versões de VDA
Autenticação de reconexão automática do cliente	Não exigir autenticação	Todas as versões de VDA
Registro em log de reconexão automática do cliente	Não registrar eventos de reconexão automática	Todas as versões de VDA
Tempo limite de reconexão automática do cliente	120 segundos	VDA 7.13 até o atual
Nível de transparência da UI 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
Limite de largura de banda de redirecionamento de dispositivo USB do cliente	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 de limite de largura de banda de redirecionamento de dispositivo USB do cliente	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 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

NOME	CONFIGURAÇÃO PADRÃO	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 multissessão e VDA para SO de sessão única
Percentual do limite de largura de banda de 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 de 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 de 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 de VDA
Limite de largura de banda de redirecionamento de impressora	0 Kbps	Todas as versões de VDA
Porcentagem de limite de largura de banda de redirecionamento de impressora	0	Todas as versões de 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

NOME	CONFIGURAÇÃO PADRÃO	VDA
		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 multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual

Redirecionamento de conteúdo bidirecional/ICA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir redirecionamento de conteúdo bidirecional	Proibido	VDA 7.13 até o atual
URLs permitidas para serem redirecionadas para o cliente	vazio	VDA 7.13 até o atual
URLs permitidas para serem redirecionadas para o VDA	vazio	VDA 7.13 até o atual
Redirecionamento de conteúdo bidirecional de cliente para host (VDA) e de cliente para cliente	Use o modelo administrativo de Objeto de Política de Grupo do aplicativo Citrix Workspace™	

Redirecionamento de conteúdo ICA/do navegador

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de conteúdo do navegador	Permitido	VDA 7.16 até o atual
Configuração de ACL de redirecionamento de conteúdo do navegador	`https://www.youtube.com/*`	VDA 7.16 até o atual
Suporte à Autenticação Integrada do Windows para	Proibido	VDA 2106 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
redirecionamento de conteúdo do navegador		
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 os 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 da área de trabalho

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de Composição da Área de Trabalho	Desabilitado (7.6 FP3 até o atual); Habilitado (5.6 até 7.6 FP2)	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Qualidade gráfica do Redirecionamento de Composição da Área de Trabalho	Médio	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Plano de fundo da área de trabalho	Permitido	Todas as versões do VDA
Animação de menu	Permitido	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Exibir conteúdo da janela ao arrastar	Permitido	Todas as versões do VDA

Monitoramento de ICA/usuário final

NOME	CONFIGURAÇÃO PADRÃO	VDA
Cálculo de ida e volta do ICA	Ativado	Todas as versões de VDA
Intervalo de cálculo de ida e volta do ICA	15 segundos	Todas as versões de VDA
Cálculos de ida e volta do ICA para conexões ociosas	Desabilitado	Todas as versões de VDA

ICA/Experiência de área de trabalho aprimorada

NOME	CONFIGURAÇÃO PADRÃO	VDA
Experiência de Área de Trabalho Aprimorada	Permitido	VDA para SO multi-sessão 7 até o atual

ICA/Redirecionamento de arquivo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conectar automaticamente unidades cliente	Permitido	Todas as versões de VDA
Redirecionamento de unidade cliente	Permitido	Todas as versões do VDA
Unidades fixas do cliente	Permitido	Todas as versões do VDA
Unidades de disquete do cliente	Permitido	Todas as versões do VDA
Unidades de rede do cliente	Permitido	Todas as versões do VDA
Unidades ópticas do cliente	Permitido	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Unidades removíveis do cliente	Permitido	Todas as versões de VDA
Redirecionamento do host para o cliente	Desabilitado	VDA para SO multissessão 7 até o atual
Preservar letras de unidade do cliente	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Acesso somente leitura à unidade do cliente	Desabilitado	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento de pasta especial	Permitido	Somente implantações do Web Interface; VDA para SO multissessão 7 até o atual
Usar gravações assíncronas	Desabilitado	Todas as versões de VDA

ICA/Gráficos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir compactação visualmente sem perdas	Desabilitado	VDA 7.6 até o atual
Limite de memória de exibição	65.536 Kb	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Preferência de degradação do modo de exibição	Degradar profundidade de cor primeiro	Todas as versões 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

NOME	CONFIGURAÇÃO PADRÃO	VDA
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 de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual
Profundidade de cor máxima permitida	32 bits por pixel	Todas as versões de VDA
Notificar o usuário quando o modo de exibição for degradado	Desabilitado	VDA para SO multissessão 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 de VDA
Compartilhamento de tela	Desabilitado	VDA 2112
Usar codec de vídeo para compactação	Usar codec de vídeo quando preferencial	VDA 7.6 FP3 até o atual
Usar codificação de hardware para codec de vídeo	Ativado	VDA 7.11 até o atual

ICA/Gráficos/Cache

NOME	CONFIGURAÇÃO PADRÃO	VDA
Limite de cache persistente	3.000.000 bps	VDA para SO multissessão 7 até o atual

ICA/Gráficos/Framehawk

NOME	CONFIGURAÇÃO PADRÃO	VDA
Canal de exibição Framehawk	Desabilitado	VDA 7.6 FP2 até o atual
Intervalo de portas do canal de exibição Framehawk	3224,3324	VDA 7.6 FP2 até o atual

ICA/Manter ativo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Tempo limite de keep alive do ICA	60 segundos	Todas as versões do VDA
Keep alives do ICA	Não enviar mensagens de keep alive do ICA	Todas as versões de VDA

ICA/Acesso a Aplicativos Locais

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir Acesso a Aplicativos Locais	Proibido	VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Lista de bloqueio de redirecionamento de URL	Nenhum site especificado	VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Lista de permissões de redirecionamento de URL	Nenhum site especificado	VDA para SO multissessão 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 multissessão 7 até o atual,

NOME	CONFIGURAÇÃO PADRÃO	VDA
		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 disponível para máquinas Windows 10 e Windows Server 2016.
Tornar a caixa de combinação remota	Proibido	VDA 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Multimídia

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de vídeo HTML5	Proibido	VDA 7.12 até o atual
Limitar qualidade de vídeo	Não configurado	VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento do Microsoft Teams	Permitido	VDA para SO de múltiplas sessões 1906 até o atual, VDA para SO de sessão única 1906 até o atual.
Conferência multimídia	Permitido	Todas as versões de VDA
Otimização para redirecionamento multimídia do Windows Media sobre WAN	Permitido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Usar GPU para otimizar o redirecionamento multimídia do Windows Media sobre WAN	Proibido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Prevenção de fallback do Windows Media	Não configurado	VDA 7.6 FP3 até o atual
Busca de conteúdo do lado do cliente do Windows Media	Permitido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento do Windows Media	Permitido	Todas as versões de VDA
Tamanho do buffer de redirecionamento do Windows Media	5 segundos	VDA 5, 5.5, 5.6 FP1 até o atual
Uso do tamanho do buffer de redirecionamento do Windows Media	Desabilitado	VDA 5, 5.5, 5.6 FP1 até o atual

Conexões ICA/Multi-Stream

NOME	CONFIGURAÇÃO PADRÃO	VDA
Áudio sobre UDP	Permitido	VDA para SO multi-sessão 7 até o atual
Intervalo de portas UDP de áudio	16500, 16509	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Política Multi-Porta	Porta primária (2598) tem Alta Prioridade	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
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 de VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo
Redirecionamento de porta LPT do cliente	Proibido	Todas as versões de VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo

ICA/Impressão

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de impressora do cliente	Permitido	Todas as versões de VDA
Impressora padrão	Definir a impressora padrão para a impressora principal do cliente	Todas as versões de VDA
Atribuições de impressora	A impressora atual do usuário é usada como impressora padrão para a sessão	Todas as versões de VDA
Preferência de log de eventos de criação automática de impressora	Registrar erros e avisos	Todas as versões VDA
Impressoras de sessão	Nenhuma impressora especificada	Todas as versões VDA
Aguardar a criação das impressoras (desktop)	Desabilitado	Todas as versões VDA

ICA/Impressão/Impressoras Cliente

NOME	CONFIGURAÇÃO PADRÃO	VDA
Criar automaticamente impressoras cliente	Criar automaticamente todas as impressoras cliente	Todas as versões VDA
Criar automaticamente impressora universal genérica	Desabilitado	Todas as versões VDA
Nomes de impressoras cliente	Nomes de impressora padrão	VDA 5.6
Conexões diretas a servidores de impressão	Ativado	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Mapeamento e compatibilidade de driver de impressora	Nenhuma regra é especificada	Todas as versões do VDA
Retenção de propriedades da impressora	Mantido no perfil somente se não for salvo no cliente	Todas as versões do 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 integrados	Ativado	Todas as versões VDA
Preferência de driver universal	EMF; XPS; PCL5c; PCL4; PS	Todas as versões VDA
Uso do driver de impressão universal	Usar impressão universal somente se o driver solicitado não estiver disponível	Todas as versões VDA

ICA/Impressão/Servidor de Impressão Universal

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar Servidor de Impressão Universal	Desabilitado	Todas as versões VDA
Porta do fluxo de dados de impressão (CGP) do Servidor de Impressão Universal	7229	Todas as versões VDA
Limite de largura de banda de entrada do fluxo de impressão do Servidor de Impressão Universal (kbps)	0	Todas as versões VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Porta do serviço web do Universal Print Server (HTTP/SOAP)	8080	Todas as versões de VDA
Universal Print Servers para balanceamento de carga	Versões de VDA 7.9 até a atual	
Limite de fora de serviço do Universal Print Server	180 (segundos)	Versões de VDA 7.9 até a atual

ICA/Impressão/Impressão Universal

NOME	CONFIGURAÇÃO PADRÃO	VDA
Modo de processamento EMF de impressão universal	Enviar diretamente para a impressora	Todas as versões de VDA
Limite de compressão de imagem de impressão universal	Melhor qualidade (compressão sem perdas)	Todas as versões de VDA
Padrões de otimização de impressão universal	Compressão de Imagem: Qualidade de imagem desejada = Qualidade padrão, Habilitar compressão pesada = Falso; Cache de Imagens e Fontes: Permitir cache de imagens incorporadas = Verdadeiro; Permitir que não administradores modifiquem essas configurações = Falso;	Todas as versões do VDA
Preferência de visualização de impressão universal	Não usar visualização de impressão para impressoras universais genéricas ou criadas automaticamente	Todas as versões do VDA
Limite de qualidade de impressão universal	Sem limite	Todas as versões do VDA

ICA/Segurança

NOME	CONFIGURAÇÃO PADRÃO	VDA
Nível mínimo de criptografia SecureICA	Básico	VDA para SO multi-sessão 7 até o atual

ICA/Limites do Servidor

NOME	CONFIGURAÇÃO PADRÃO	VDA
Intervalo do temporizador de inatividade do servidor	0 milissegundos	VDA para SO multi-sessão 7 até o atual

Limites de ICA/Sessão

NOME	CONFIGURAÇÃO PADRÃO	VDA
Temporizador de sessão desconectada	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Temporizador de sessão desconectada do Acesso Remoto para PC	Desabilitado	VDA para SO de sessão única 7 até o atual
Intervalo do temporizador de sessão desconectada	1.440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Temporizador de conexão de sessão	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Intervalo do temporizador de conexão de sessão	1.440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Temporizador de inatividade da sessão	Ativado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
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

Controle de ICA/Fuso Horário

NOME	CONFIGURAÇÃO PADRÃO	VDA
Estimar hora local para clientes legados	Ativado	VDA para SO multi-sessão 7 até o atual
Restaurar fuso horário do SO de sessão única na desconexão ou logoff da sessão	Ativado	Versão atual do VDA
Usar hora local do cliente	Usar fuso horário do servidor	Todas as versões do VDA

Dispositivos ICA/TWAIN

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de dispositivo TWAIN do cliente	Permitido	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
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 é 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 preferencial para gráficos simples	24 bits por pixel	VDA 7.6 FP3 até o atual
Taxa de quadros de destino	30 quadros por segundo	Todas as versões do 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
Compactação 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 compactação progressiva	2,147,483,647 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Taxa de quadros mínima alvo	10 quadros por segundo	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Exibição Visual/Imagens Estáticas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Compressão de cor extra	Desabilitado	Todas as versões de VDA
Limite de compressão de cor extra	8,192 Kbps	Todas as versões de VDA
Compressão pesada	Desabilitado	Todas as versões de VDA
Nível de compressão com perdas	Médio	Todas as versões de VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Valor limite de compressão com perdas	2,147,483,647 Kbps	Todas as versões de VDA

ICA/WebSockets

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conexões WebSockets	Proibido	VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Número da porta WebSockets	8008	VDA para SO multissessão 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 todas as URLs do Receiver para Web	VDA para SO multissessão 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 multissessão 7 até o atual
Uso da CPU	Desabilitado	VDA para SO multi-sessão 7 até o atual
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 multi-sessão 7 até o atual
Número máximo de sessões	250	VDA para SO multi-sessão 7 até o atual
Uso de memória	Desabilitado	VDA para SO multi-sessão 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Carga base de uso de memória	Carga zero: 768 MB	VDA para SO multi-sessão 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 Perfil/Configurações básicas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Gravação ativa	Desabilitado	Todas as versões de VDA
Habilitar Gerenciamento de Perfil	Desabilitado	Todas as versões de VDA
Grupos excluídos	Desabilitado. Membros de todos os grupos de usuários são processados.	Todas as versões de VDA
Suporte a perfil offline	Desabilitado	Todas as versões VDA
Caminho para o armazenamento do usuário	Windows	Todas as versões VDA
Processar logons de administradores locais	Desabilitado	Todas as versões VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Grupos processados	Desabilitado. Membros de todos os grupos de usuários são processados.	Todas as versões VDA

Gerenciamento de Perfil/Configurações entre Plataformas

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 VDA
Habilitar configurações de plataforma cruzada	Desabilitado	Todas as versões VDA
Caminho para definições de plataforma cruzada	Desativado. Nenhum caminho é especificado.	Todas as versões de VDA
Caminho para o armazenamento de configurações multiplataforma	Desativado. Windows\PM_CM é usado.	Todas as versões de VDA
Fonte para criar configurações multiplataforma	Desabilitado	Todas as versões de VDA

Gerenciamento de Perfil/Sistema de Arquivos/Exclusões

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de exclusão - diretórios	Desativado. Todas as pastas no perfil do usuário são sincronizadas.	Todas as versões de VDA
Lista de exclusão - arquivos	Desativado. Todos os arquivos no perfil do usuário são sincronizados.	Todas as versões de VDA

Gerenciamento de Perfil/Sistema de Arquivos/Sincronização

NOME	CONFIGURAÇÃO PADRÃO	VDA
Diretórios para sincronizar	Desabilitado. 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)	Desativado. Nenhum local é especificado.	Todas as versões do VDA
Configurações de redirecionamento para AppData(Roaming)	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho do AppData(Roaming)	Todas as versões do VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Contatos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Contatos	Desativado. Nenhum local é especificado.	Todas as versões do VDA
Configurações de redirecionamento para Contatos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Contatos**	Todas as versões do VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Área de Trabalho

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho da Área de Trabalho	Desativado. Nenhuma localização é especificada.	Todas as versões de 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 dos documentos	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Documentos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Documentos**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Downloads

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos downloads	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Downloads	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Downloads**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Favoritos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Favoritos	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 de 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
Configurações de redirecionamento para Links	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Links**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Música

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho da Música	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Música	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Música**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Imagens

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho das Imagens	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Imagens	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Imagens**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Jogos Salvos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho de Jogos Salvos	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Jogos Salvos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Jogos Salvos**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Pesquisas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho de Pesquisas	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Pesquisas	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Pesquisas**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Menu Iniciar

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do Menu Iniciar	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para o Menu Iniciar	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho do Menu Iniciar	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Vídeo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do vídeo	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Vídeo	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho do vídeo**	Todas as versões de VDA

Configurações de Gerenciamento de Perfil/Log

NOME	CONFIGURAÇÃO PADRÃO	VDA
Ações do Active Directory	Desabilitado	Todas as versões de VDA
Informações comuns	Desabilitado	Todas as versões de VDA
Avisos comuns	Desabilitado	Todas as versões de VDA
Habilitar registro em log	Desabilitado	Todas as versões de VDA
Ações do sistema de arquivos	Desabilitado	Todas as versões de VDA
Notificações do sistema de arquivos	Desabilitado	Todas as versões de VDA
Logoff	Desabilitado	Todas as versões de VDA
Logon	Desabilitado	Todas as versões de VDA
Tamanho máximo do arquivo de log	1048576	Todas as versões de VDA
Caminho para o arquivo de log	Desabilitado. Os arquivos de log são salvos no local padrão; %SystemRoot% \System32\Logfiles\UserProfileManager.	Todas as versões de VDA
Informações personalizadas do usuário	Desabilitado	Todas as versões de VDA
Valores da política no logon e logoff	Desabilitado	Todas as versões de VDA
Ações do Registro	Desabilitado	Todas as versões de VDA
Diferenças do Registro no logoff	Desabilitado	Todas as versões de VDA

Gerenciamento de perfil/Manipulação de perfil

NOME	CONFIGURAÇÃO PADRÃO	VDA
Atraso antes de excluir perfis em cache	0	Todas as versões de VDA
Excluir perfis armazenados em cache localmente no logoff	Desabilitado	Todas as versões de VDA
Tratamento de conflitos de perfil local	Usar perfil local	Todas as versões de VDA
Migração de perfis existentes	Local e roaming	Todas as versões de VDA
Caminho para o perfil de modelo	Desabilitado. Novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.	Todas as versões de VDA
Perfil de modelo substitui perfil local	Desabilitado	Todas as versões de VDA
Perfil de modelo substitui perfil móvel	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

NOME	CONFIGURAÇÃO PADRÃO	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 Perfil/Perfis de usuário transmitidos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Sempre armazenar em cache	Desabilitado	Todas as versões de VDA
Tamanho do cache permanente	0 Mb	Todas as versões de VDA
Streaming de perfil	Desabilitado	Todas as versões de VDA
Grupos de perfis de usuário transmitidos	Desativado. Todos os perfis de usuário dentro de uma OU são processados normalmente.	Todas as versões de VDA
Tempo limite para arquivos de bloqueio de área pendentes (dias)	1 dia	Todas as versões de VDA

Receiver

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de contas do StoreFront™	Nenhuma loja especificada	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

Camada de personalização do usuário

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do Repositório da Camada de Usuário	Desabilitado. Nenhum caminho especificado.	VDA 19.12 e versões posteriores

NOME	CONFIGURAÇÃO PADRÃO	VDA
Tamanho da Camada de Usuário em GB	10 GB. Uma camada de usuário é um disco com provisionamento dinâmico que se expande até o tamanho definido. As camadas de usuário nunca diminuem de tamanho.	VDA 19.12 ou versões posteriores

Virtual Delivery Agent

NOME	CONFIGURAÇÃO PADRÃO	VDA
Máscara de rede IPv6 de registro do Controller	Nenhuma máscara de rede é especificada	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Porta de registro do Controller	80	Todas as versões do VDA
SIDs do Controller	Nenhum SID é especificado	Todas as versões de VDA
Controladores	Nenhum controlador é especificado	Todas as versões de VDA
Habilitar atualização automática de controladores	Ativado	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Usar apenas registro de controlador IPv6	Desabilitado	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
GUID do site	Nenhum GUID é especificado	Todas as versões de VDA

Virtual Delivery Agent/HDX 3D Pro

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar sem perdas	Ativado	VDA 5.5, 5.6 FP1

NOME	CONFIGURAÇÃO PADRÃO	VDA
Configurações de qualidade do HDX 3D Pro	VDA 5.5, 5.6 FP1	

Virtual Delivery Agent/Monitoramento

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar monitoramento de processo	Desabilitado	VDA 7.11 até o atual
Habilitar monitoramento de recursos	Ativado	VDA 7.11 até o atual

IP virtual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Suporte a loopback de IP virtual	Desabilitado	VDA 7.6 até o atual
Lista de programas de loopback virtual de IP virtual	Nenhum	VDA 7.6 até o atual

Referência de configurações de política

As políticas incluem configurações que são aplicadas quando a política é imposta. As descrições nesta seção também indicam se mais configurações são necessárias para habilitar um recurso ou se são semelhantes a uma configuração.

Referência rápida

As tabelas a seguir listam as configurações que você pode configurar dentro de uma política. Encontre a tarefa que você deseja concluir na coluna esquerda e, em seguida, localize a configuração correspondente na coluna 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) é 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 de áudio
Controlar o mapeamento de áudio para alto-falantes no dispositivo do usuário	Redirecionamento de áudio do cliente

Largura de banda para dispositivos de usuário

PARA LIMITAR A LARGURA DE BANDA USADA PARA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Mapeamento de áudio do cliente	Limite de largura de banda de redirecionamento de áudio ou porcentagem do limite de largura de banda de redirecionamento de áudio
Recortar e colar usando uma área de transferência local	Limite de largura de banda de redirecionamento da área de transferência ou porcentagem do limite de largura de banda de redirecionamento da área de transferência
Acesso em uma sessão a unidades de cliente locais	Limite de largura de banda de redirecionamento de arquivo ou porcentagem do limite de largura de banda de redirecionamento de arquivo
Aceleração Multimídia HDX™ MediaStream	Limite de largura de banda de Aceleração Multimídia HDX MediaStream ou porcentagem do limite de largura de banda de Aceleração Multimídia HDX MediaStream
Sessão do cliente	Limite geral de largura de banda da sessão

PARA LIMITAR A LARGURA DE BANDA USADA PARA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Impressão	Limite de largura de banda de redirecionamento de impressora ou porcentagem do limite de largura de banda de redirecionamento de impressora
Dispositivos TWAIN (como uma câmera ou scanner)	Limite de largura de banda de redirecionamento de dispositivo TWAIN ou porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN
Dispositivos USB	Limite de largura de banda de redirecionamento de dispositivo USB do cliente ou porcentagem do limite de largura de banda de redirecionamento de dispositivo USB do cliente

Redirecionamento de unidades de cliente e dispositivos de usuário

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se as unidades no dispositivo do usuário são conectadas quando os usuários fazem logon no servidor ou não	Conectar automaticamente unidades cliente
Controla a transferência de dados de recortar e colar entre o servidor e a área de transferência local	Redirecionamento da área de transferência do cliente
Controla como as unidades são mapeadas do dispositivo do usuário	Redirecionamento de unidade cliente
Controla se os discos rígidos locais dos usuários estão disponíveis em uma sessão	Unidades fixas do cliente e redirecionamento de unidade do cliente
Controla se as unidades de disquete locais dos usuários estão disponíveis em uma sessão	Unidades de disquete do cliente e redirecionamento de unidade do cliente
Controla se as unidades de rede dos usuários estão disponíveis em uma sessão	Unidades de rede do cliente e redirecionamento de unidade do cliente

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se as unidades de CD, DVD ou Blu-ray locais dos usuários estão disponíveis em uma sessão	Unidades ópticas do cliente e redirecionamento de unidade do cliente
Controla se as unidades removíveis locais dos usuários estão disponíveis em uma sessão	Unidades removíveis do cliente e redirecionamento de unidade do cliente
Controla se os dispositivos TWAIN dos usuários, como scanners e câmeras, estão disponíveis em uma sessão e controla a compactação das transferências de dados de imagem	Redirecionamento de dispositivo TWAIN do cliente; redirecionamento de compactação TWAIN
Controla se os dispositivos USB estão disponíveis em uma sessão	Redirecionamento de dispositivo USB do cliente e regras de redirecionamento de dispositivo USB do cliente
Melhora a velocidade de gravação e cópia de arquivos para um disco cliente em uma WAN	Usar gravações assíncronas

Redirecionamento de conteúdo

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se deve usar o redirecionamento de conteúdo do servidor para o dispositivo do usuário	Redirecionamento do host para o cliente

UI da Área de Trabalho

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar se o papel de parede da área de trabalho é usado nas sessões dos usuários ou não	Papel de parede da área de trabalho
Visualizar o conteúdo da janela enquanto uma janela é arrastada	Visualizar o conteúdo da janela ao arrastar

Gráficos e multimídia

Importante:

A política do Flash permanece apenas para permitir que clientes com VDAs mais antigos usem controladores mais recentes (por exemplo, controladores da versão 1912) e ainda usem o Flash. Esta versão do VDA não oferece suporte ao Flash.

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar o número máximo de quadros por segundo enviados para dispositivos de usuário a partir de desktops virtuais	Taxa de quadros de destino
Controlar a qualidade visual das imagens exibidas no dispositivo do usuário	Qualidade visual
Controlar se os sites podem exibir conteúdo Flash quando acessados em sessões	Lista de URLs de busca de conteúdo Flash do lado do servidor; Lista de compatibilidade de URL Flash; Configuração de política de prevenção de fallback de vídeo Flash; Erro de prevenção de fallback de vídeo Flash *.swf
Controlar a compactação de vídeo renderizado no servidor	Usar codec de vídeo para compactação; Usar codificação de hardware para codec de vídeo
Controlar a entrega de conteúdo web multimídia HTML5 aos usuários	Redirecionamento de vídeo HTML5

Priorizar o tráfego de rede Multi-Stream

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Especificar portas para tráfego ICA® em várias conexões e estabelecer prioridades de rede	Política de Multiportas

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Habilitar suporte para conexões de múltiplos fluxos 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 embutidos
Controlar quando usar o Driver de Impressora Universal	Uso do driver de impressão universal
Escolher uma impressora com base nas informações da sessão de usuário em roaming	Impressora padrão
Balancear carga e definir limite de failover para Servidores de Impressão Universais	Servidores de Impressão Universal para balanceamento de carga; Limite de fora de serviço dos Servidores de Impressão Universal

Observação:

> As políticas não podem ser usadas para habilitar um protetor de tela em uma sessão de área de trabalho ou aplicativo. Para usuários que exigem protetores de tela, o protetor de tela pode ser implementado no dispositivo do usuário.

Configurações de política ICA®

> **Observação:**

> Esta página fornece descrições e valores de configuração suportados para as configurações de política ICA. Para obter mais informações sobre como trabalhar com políticas, consulte a seção Trabalhar com políticas.

Transporte adaptável

Essa configuração permite ou impede o transporte de dados via EDT como primário e o fallback para TCP.

Por padrão, o transporte adaptável está ativado (**Preferencial**), e o EDT é usado quando possível, com fallback para TCP. Se ele foi desativado e você deseja ativá-lo, siga este procedimento.

1. No Studio, habilite a configuração de política, transporte adaptável HDX™. Também recomendamos que você não habilite esse recurso como uma política universal para todos os objetos no Site.
2. Para habilitar a configuração de política, defina o valor como **Preferencial** e clique em **OK**.

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 essa configuração apenas para solução de problemas.

Desativado. O TCP é forçado e o EDT é desativado.

Para obter mais informações, consulte Transporte adaptável.

Configuração de arrastar e soltar

Essa configuração permite ou impede o arrastar de arquivos entre o cliente e aplicativos ou desktops virtuais. Por padrão, a política de arrastar e soltar está desabilitada. Para habilitar essa política, faça o seguinte:

1. No Citrix Studio, habilite a configuração de política, **Arrastar e soltar**.
2. Defina o valor como **Habilitado** e clique em **OK**.

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 esse 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 impedir a transferência de dados de recortar e colar entre uma sessão e a área de transferência local, selecione **Proibir**. Os usuários ainda podem recortar e colar dados entre aplicativos em execução nas sessões.

Depois de permitir esta configuração, configure a largura de banda máxima permitida que a área de transferência pode consumir em uma conexão de cliente. Use as configurações **Limite de largura de banda de redirecionamento da área de transferência** ou **Porcentagem do limite de largura de banda de redirecionamento da área de transferência**.

Formatos permitidos para gravação na área de transferência do cliente

Quando a configuração **Restringir gravação na área de transferência do cliente** estiver **Habilitada**, os dados da área de transferência do host não poderão 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 em 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.

Limitar o tamanho da transferência da área de transferência do cliente para a sessão

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de um endpoint cliente para uma sessão virtual durante uma única operação de recortar 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, essa configuração está desabilitada e não há limite para transferências do cliente para a sessão.

Limitar o tamanho da transferência da área de transferência da sessão para o cliente

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de uma sessão virtual para um endpoint cliente durante uma única operação de recortar e colar.

Para limitar o tamanho da transferência da área de transferência, habilite a configuração **Limitar o tamanho da transferência da área de transferência da sessão para o cliente**. Em seguida, no campo **Limite de Tamanho**, insira um valor em kilobytes para definir o tamanho da transferência de dados entre uma sessão e a área de transferência local.

Por padrão, essa configuração está desabilitada e não há limite para transferências da sessão para o cliente.

Restringir a gravação da área de transferência do cliente

Se essa configuração estiver **Habilitada**, os dados da área de transferência do host não poderão ser compartilhados com o endpoint cliente. Você pode permitir formatos específicos habilitando a configuração **Formatos permitidos para gravação da área de transferência do cliente**.

Por padrão, essa configuração está **Desabilitada**.

Restringir a gravação da área de transferência da sessão

Quando essa 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 **Formatos permitidos para gravação da área de transferência da sessão**.

Por padrão, essa configuração está **Desabilitada**.

Formatos permitidos para gravação na área de transferência da sessão

Quando a configuração **Restringir gravação na área de transferência da sessão** está **Habilitada**, os dados da área de transferência do cliente não podem ser compartilhados com os aplicativos da sessão. Você pode usar essa 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.

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 da sessão** estiver definida como **Desabilitado**.

> **Observação:**
>
> A habilitação do 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.

Início da área de trabalho

Essa 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 do VDA que estão usando uma conexão RDP. Esses usuários podem se conectar ao VDA quando essa configuração está habilitada ou desabilitada. Essa configuração não afeta usuários não administrativos que não estão em um grupo de Usuários de Acesso Direto do VDA. Esses usuários não podem se conectar ao VDA quando essa configuração está habilitada ou desabilitada.

Redirecionamento FIDO2

Essa configuração habilita ou desabilita 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 está **Permitida**.

O redirecionamento FIDO2 também pode ser habilitado ou desabilitado em endpoints de cliente configurando a seguinte chave de registro:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\

Nome: FIDO2

Tipo: REG_DWORD

Valor: 1

Defina o valor como 0 para desativar o recurso e 1 para ativá-lo. Por padrão, o recurso está ativado.

> **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. Certifique-se de fazer backup do registro antes de editá-lo.

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 conhecidos. Se você alterar o número da porta, reinicie o

servidor para que o novo valor entre em vigor. Se você alterar o número da porta no servidor, também deverá alterá-lo em cada aplicativo ou plug-in Citrix Workspace™ que se conecta ao servidor.

Teclado e Editor de Método de Entrada (IME)

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 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.

   Suporte à sincronização dinâmica do layout do teclado do cliente - ativa a sincronização dinâmica do layout do teclado.

   Suporte à sincronização dinâmica do layout do teclado do cliente e melhoria do IME - habilita a sincronização dinâmica do layout do teclado e 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 sendo sincronizado 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**
  - Desativado no Windows Server 2016 e Windows Server 2019.

    - Suporte à 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 de 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 estiver disponível.
> - O modo tolerante a perdas 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.

Por padrão, o modo tolerante a perdas 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.

Para obter mais informações, consulte Modo tolerante a perdas.

Limites tolerantes a perdas

Quando o modo tolerante a perdas estiver disponível, esta configuração especifica os limites das métricas de rede nos quais a sessão muda para o modo tolerante a perdas.

Os limites padrão são:

- Perda de pacotes: 5%
- Latência: 300 ms (RTT)

Para obter mais informações, consulte Modo tolerante a perdas.

Protocolo Rendezvous

Essa configuração altera como as sessões HDX são proxyadas ao usar o Citrix Gateway Service. Quando ativado, 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 ativado por padrão, enquanto a configuração HDX é desativada 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 ativada.

Por padrão, essa configuração está desativada.

Quando desativado, o VDA não roteia o tráfego de saída através de proxies não transparentes ao tentar estabelecer uma conexão Rendezvous com o Gateway Service.

Quando ativado, o VDA tenta estabelecer uma conexão Rendezvous com o Gateway Service através do proxy definido nesta configuração.

O VDA suporta o uso de proxies HTTP e SOCKS5 para conexões Rendezvous. Para configurar o VDA para usar um proxy para a conexão Rendezvous, você deve ativar 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 suportada para configuração de proxy com um arquivo PAC. Para obter mais informações sobre o esquema de arquivo PAC para proxies SOCKS5, consulte Configuração de proxy.

> **Observação:**
>
> Somente proxies SOCKS5 suportam transporte de dados via EDT. Para um proxy HTTP, use TCP como protocolo de transporte para ICA.

> Para obter mais informações, consulte Protocolo Rendezvous.

Início de programas não publicados durante a conexão do cliente

Esta configuração especifica se deve permitir o início de aplicativos iniciais via RDP no servidor.

Por padrão, o início de aplicativos iniciais via RDP no servidor não é permitido.

Configurações de política de alternância do modo tablet

A alternância do modo tablet otimiza a aparência e o comportamento dos aplicativos da Store, aplicativos Win32 e do shell do Windows no VDA. Isso é feito alternando automaticamente o desktop 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 aplicativo Citrix Workspace™ contendo a chave para o ID da sessão e as credenciais não for usado, a reconexão automática poderá resultar no início de uma nova sessão. Ou seja, em vez de reconectar a uma sessão existente. O cookie não é usado se tiver expirado. Por exemplo, o cookie pode expirar devido a um atraso na reconexão, ou se as credenciais precisarem ser reinseridas. Se os usuários se desconectarem intencionalmente, a reconexão automática do cliente não será acionada.

Uma janela de sessão fica esmaecida quando uma reconexão está em andamento. Um temporizador de contagem regressiva exibe o tempo restante antes que a sessão seja reconectada. Quando uma sessão expira, ela é desconectada.

Para sessões de aplicativo, quando a reconexão automática é permitida, um temporizador de contagem regressiva aparece na área de notificação. Este temporizador especifica o tempo restante antes que a sessão seja reconectada. O aplicativo Citrix Workspace tenta reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de usuário, quando a reconexão automática é permitida, o aplicativo Citrix Workspace tenta reconectar à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, este período é de dois minutos. Para alterar este período, edite a política.

Por padrão, a reconexão automática do cliente é permitida.

Para desabilitar a reconexão automática do cliente:

1. Inicie o Citrix Studio.
2. Abra a política de **Reconexão automática do cliente**.
3. Defina a política como **Proibida**.

Imagem de reconexão automática do cliente(/en-us/xenapp-and-xendesktop/current-release/media/auto-client-reconnect.png)

Autenticação de reconexão automática do cliente

Essa configuração exige autenticação 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 aplicativo Citrix Workspace. Quando essa configuração é configurada, os cookies não são usados. Em vez disso, uma caixa de diálogo é exibida aos usuários solicitando credenciais quando o aplicativo Citrix Workspace tenta se reconectar automaticamente.

Por padrão, a autenticação não é necessária.

Para alterar a autenticação de reconexão automática do cliente:

1. Inicie o Citrix Studio.
2. Abra a política de **autenticação de reconexão automática do cliente**.
3. Habilite ou desabilite a autenticação.
4. Escolha **OK**.

Registro de reconexão automática do cliente

Essa configuração habilita ou desabilita o registro de reconexões automáticas do cliente no log de eventos.

Quando o registro está habilitado, o Log do Sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Um site não fornece um log combinado de eventos de reconexão para todos os servidores.

Por padrão, o registro está desabilitado.

Para alterar o registro de reconexão automática do cliente:

1. Iniciar o Citrix Studio.
2. Abra a política de **registro de reconexão automática do cliente**.
3. Ative ou desative o registro.
4. Escolha **OK**.

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.

Para alterar o tempo limite de reconexão automática do cliente:

1. Iniciar o Citrix Studio.
2. Abra a política de **tempo limite de reconexão automática do cliente**.
3. Edite o valor do tempo limite.
4. Escolha **OK**.

Nível de transparência da interface do usuário de reconexão

Você pode usar a política do Studio para configurar 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%.

Para alterar o nível de opacidade da interface do usuário de reconexão:

1. Iniciar o Citrix Studio.
2. Abra a política de **Nível de transparência da interface do usuário de reconexão**.
3. Edite o valor.
4. Escolha **OK**.

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

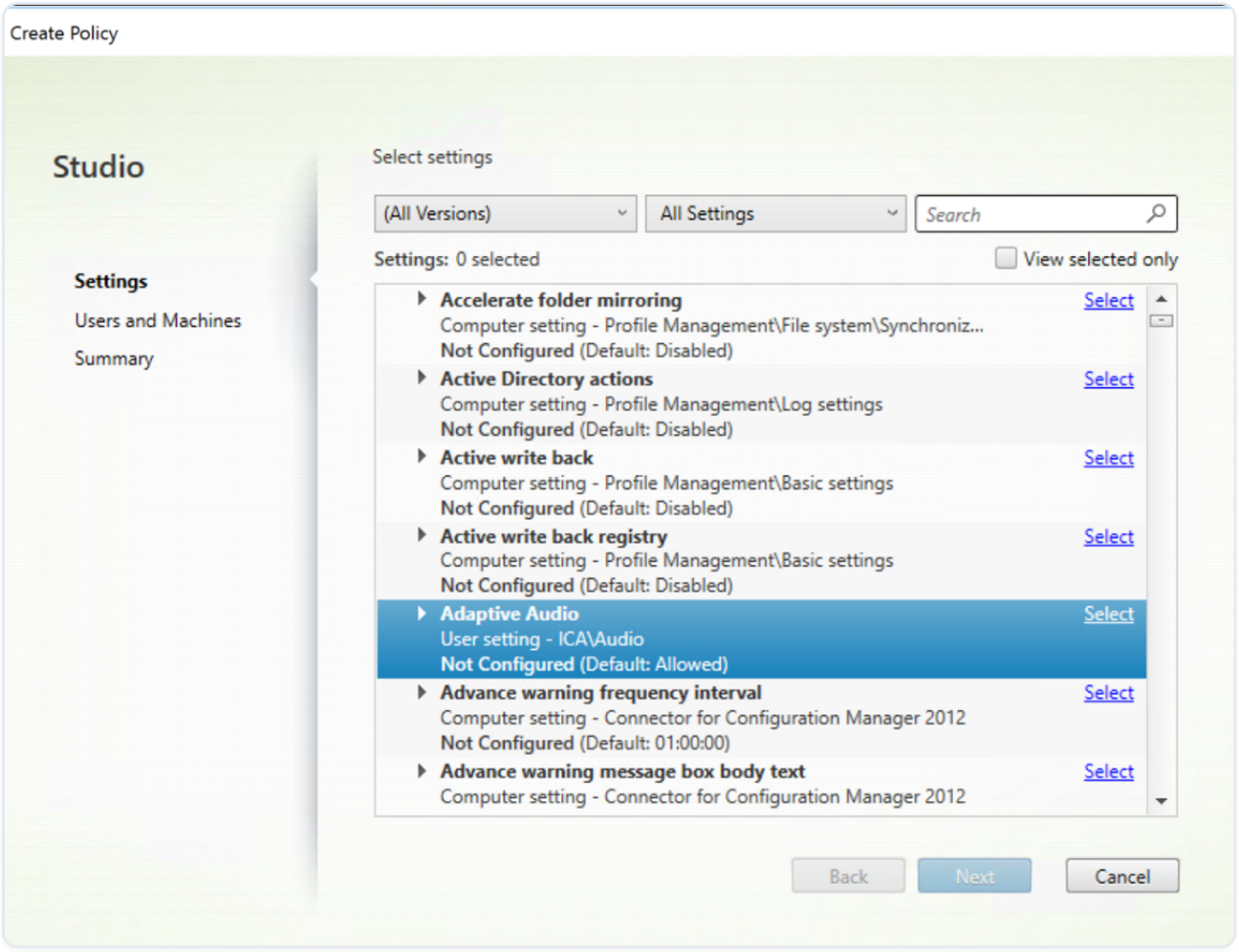
Esta configuração habilita ou desabilita o áudio adaptável. Ao habilitar esta política, as configurações de qualidade de áudio são ajustadas dinamicamente para fornecer a melhor experiência do usuário. Esta configuração se aplica a sessões de SO de sessão única e SO de múltiplas sessões de VDAs usando Citrix Virtual Apps and Desktops™ 2109 ou posterior.

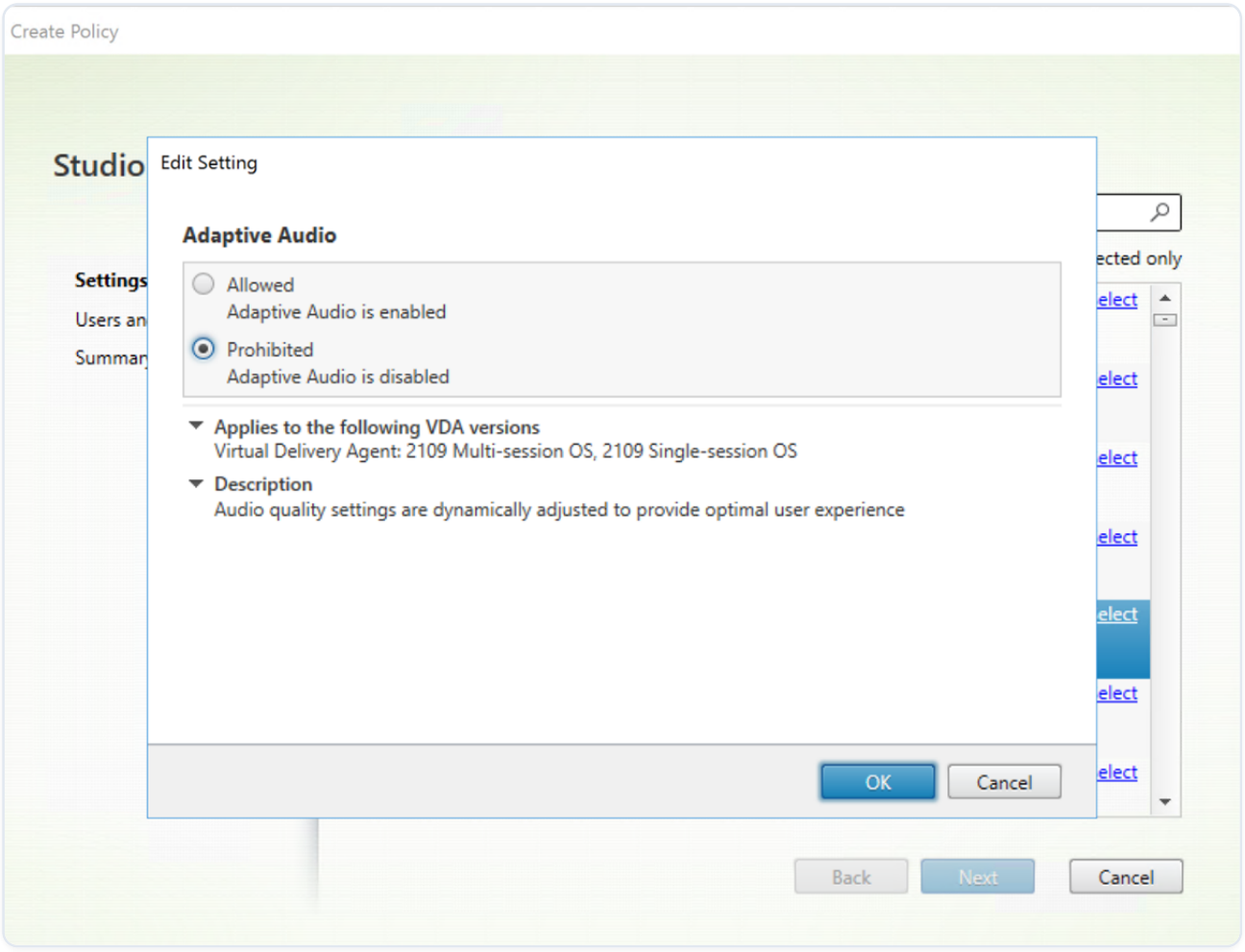
Quando esta configuração é proibida, a política de qualidade de áudio é aplicada. Para obter mais informações, consulte Qualidade de áudio.

Por padrão, a política de áudio adaptável está habilitada.

Para desabilitar o áudio adaptável:

1. Inicie o Citrix Studio.
2. Abra a política de **Áudio Adaptável**.
3. Defina a política como **Proibida**.





Áudio sobre transporte em tempo real UDP

Esta configuração permite ou impede a transmissão e o recebimento de áudio entre o VDA e o dispositivo do usuário via RTP usando o Protocolo de Datagrama de Usuário (UDP). Quando esta configuração é desabilitada, o áudio é enviado e recebido via TCP.

Por padrão, o áudio sobre UDP é permitido.

Plug N Play de áudio

Esta configuração permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som.

Por padrão, o uso de vários dispositivos de áudio é permitido.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Qualidade do áudio

Esta configuração especifica o nível de qualidade do som recebido nas sessões do usuário.

Por padrão, a qualidade do som é definida como Alta - áudio de alta definição.

Para controlar a qualidade do som, escolha uma das seguintes opções:

- Selecione Baixa - para conexões de baixa velocidade para conexões de baixa largura de banda. Os sons enviados para o dispositivo do usuário são compactados em até 16 Kbps. Essa compactação resulta em uma redução significativa na qualidade do som. Mas também permite um desempenho razoável para uma conexão de baixa largura de banda.
- Selecione Média - otimizada para fala para fornecer aplicativos de Voz sobre Protocolo de Internet. Esta configuração oferece 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 fornecer 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 **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem do limite de largura de banda de redirecionamento de áudio**.

Redirecionamento de áudio do cliente

Esta configuração especifica se os aplicativos hospedados no servidor podem reproduzir sons através de um dispositivo de som instalado no dispositivo do usuário. Esta 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 a quantidade de largura de banda utilizada pelo áudio pode melhorar o desempenho do aplicativo, mas também pode degradar a qualidade do áudio. Ela é consumida apenas enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo dela dobra. Para especificar a quantidade máxima de largura de banda, configure as definições **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem do limite de largura de banda de redirecionamento de áudio**.

Em máquinas Windows Multi-session OS, certifique-se de que a configuração **Audio Plug N Play** esteja habilitada para suportar múltiplos dispositivos de áudio.

Importante: Proibir o redirecionamento de áudio do cliente desabilita toda a funcionalidade de áudio HDX™.

Redirecionamento de microfone do cliente

Esta configuração habilita ou desabilita o redirecionamento do microfone do cliente. Quando habilitado, os usuários podem usar microfones para gravar entrada de áudio em uma sessão.

Por padrão, o redirecionamento de microfone é permitido.

Por segurança, os usuários são alertados quando servidores não confiáveis por seus dispositivos tentam acessar microfones. Os usuários podem escolher aceitar ou não aceitar o acesso. Os usuários podem desabilitar o alerta no aplicativo Citrix Workspace™.

Em máquinas Windows Multi-session OS, certifique-se de que a configuração Audio Plug N Play esteja Habilitada para suportar múltiplos dispositivos de áudio.

Se a configuração **Redirecionamento de áudio do cliente** estiver desabilitada no dispositivo do usuário, esta regra não terá efeito.

Configurações de política de largura de banda

A seção **Largura de banda** inclui configurações de política para evitar problemas de desempenho relacionados ao uso da largura de banda da sessão do cliente.

Importante: O uso dessas configurações de política com as configurações da **política Multi-Stream** pode produzir resultados inesperados. Se você usar as configurações Multi-Stream em uma política, certifique-se de que essas configurações de política de limite de largura de banda não estejam incluídas.

Limite de largura de banda de redirecionamento de áudio

Esta configuração especifica a largura de banda máxima permitida para reprodução ou gravação de áudio em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de áudio

Esta configuração especifica o limite máximo de largura de banda permitido para reprodução ou gravação de áudio como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para as sessões do cliente.

Limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB para e do cliente. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de dispositivo USB do cliente**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB de e para o cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **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 Configure COM Port and LPT Port Redirection settings using the registry.

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 registo; consulte Configurar as definições de Redirecionamento de Porta COM e Porta LPT usando o registo.

Esta definição especifica a largura de banda máxima permitida para aceder a portas COM numa ligação de cliente como uma percentagem da largura de banda total da sessão.

Por predefinição, nenhum máximo (zero) é especificado

Se introduzir um valor para esta definição e um valor para a definição **Limite de largura de banda de redirecionamento de porta COM**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se configurar esta definição, também deve configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente

Limite de largura de banda de redirecionamento de ficheiros

Esta definição especifica a largura de banda máxima permitida para aceder a uma unidade de cliente numa sessão de utilizador. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por predefinição, nenhum máximo (zero) é especificado.

Se introduzir um valor para esta definição e um valor para a definição **Percentagem do limite de largura de banda de redirecionamento de ficheiros**, a definição mais restritiva (o valor mais baixo) entra em vigor.

Porcentagem de limite de largura de banda de redirecionamento de arquivo

Esta definição especifica o limite máximo de largura de banda permitido para aceder a unidades de cliente como uma percentagem da largura de banda total da sessão.

Por predefinição, nenhum máximo (zero) é especificado.

Se introduzir um valor para esta definição e um valor para a definição **Limite de largura de banda de redirecionamento de ficheiros**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se configurar esta definição, também deve configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Limite de largura de banda de aceleração multimédia HDX™ MediaStream

Esta definição especifica o limite máximo de largura de banda permitido para a entrega de áudio e vídeo em streaming usando a Aceleração Multimédia HDX MediaStream. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) terá efeito.

Porcentagem do limite de largura de banda da aceleração multimídia HDX MediaStream

Esta configuração especifica a largura de banda máxima permitida para a entrega de áudio e vídeo 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 as sessões do 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 de largura de banda geral 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) é aplicada.

Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN

Esta configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN de aplicativos publicados como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de dispositivo TWAIN**, a configuração mais restritiva (com o valor mais baixo) é aplicada.

Se você configurar esta definição, você também deve 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** contém configurações de política para habilitar ou desabilitar o redirecionamento de URL do cliente para o host e do host para o cliente.

As políticas de servidor são definidas no Studio. 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 do host para o cliente e Acesso a Aplicativos Locais para redirecionamento do cliente para URL. No entanto, recomendamos que você use o redirecionamento de conteúdo bidirecional para clientes Windows ingressados no domínio.

Permitir Redirecionamento de Conteúdo Bidirecional

Defina esta política como **Permitido** para habilitar o redirecionamento entre o servidor (VDA) e o cliente. Por padrão, ela é definida como **Proibido**.

Use a política **URLs permitidas para serem redirecionadas para o cliente** para configurar a lista de URLs para redirecionamento do VDA para o cliente.

> **Observação:**
>
> Esta política deve ser definida com a política **Redirecionamento de Conteúdo Bidirecional** no cliente para que o redirecionamento seja permitido.

URLs permitidas para serem redirecionadas para o Cliente

Especifica a lista de URLs a serem abertas no cliente quando o redirecionamento de conteúdo bidirecional é permitido.

Um ponto e vírgula (;) é o delimitador. Um asterisco (*) pode ser usado como um curinga. Por exemplo:

```
*.xyz.com;https://www.example.com
```

Configurações de política de redirecionamento de conteúdo do navegador

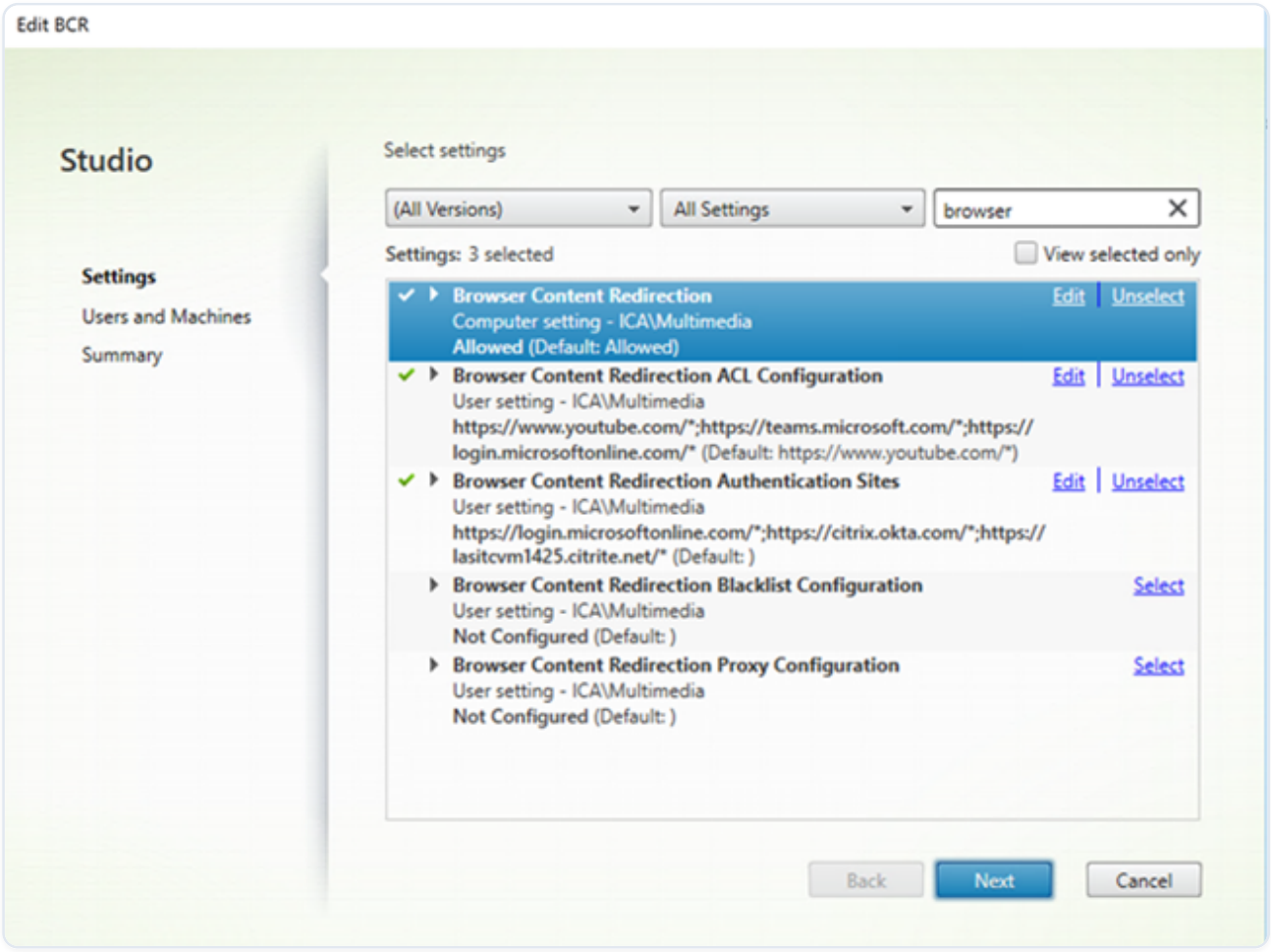
A seção de redirecionamento de conteúdo do navegador inclui configurações de política para configurar esse recurso.

O redirecionamento de conteúdo do navegador controla e otimiza a forma como o Citrix Virtual Apps and Desktops™ entrega qualquer conteúdo do 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 Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX é usado para o redirecionamento de conteúdo do navegador. Para obter mais informações, consulte Redirecionamento de conteúdo do navegador.

Configurações de política:

As seguintes configurações de política estão disponíveis para o recurso de redirecionamento de conteúdo do navegador no Citrix Studio. Essas políticas podem ser substituídas por chaves de registro no VDA, mas as chaves de registro são opcionais.



TLS e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) em execução no VDA.

Para conseguir esse redirecionamento e manter a integridade TLS da página da web, o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX gera dois certificados personalizados no armazenamento de certificados no VDA.

HdxVideo.js usa Web sockets seguros para se comunicar com o WebSocketService.exe em execução no VDA. Esse processo é executado no Sistema Local e realiza a terminação SSL e o mapeamento da sessão do usuário.

WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

Redirecionamento de conteúdo do navegador

Por padrão, o aplicativo Citrix Workspace™ tenta a busca e a renderização do cliente. A renderização do lado do servidor é tentada quando a busca e a renderização do cliente falham. Se você também habilitar a política de configuração de proxy de redirecionamento de conteúdo do navegador, o aplicativo Citrix Workspace tentará apenas a busca do servidor e a renderização do cliente.

Por padrão, essa configuração é Permitida.

Configuração de suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

A redireção de conteúdo do navegador permite 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 VDA do usuário. O usuário então se autentica no servidor web com 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. Esse método de autenticação exige que os usuários insiram suas credenciais VDA cada vez que acessam o servidor web.

Por padrão, essa configuração é Proibida.

Configuração de autenticação de proxy web de busca do servidor de redirecionamento de conteúdo do navegador

Essa 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 a redireção de conteúdo do navegador para o modo de busca do 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 de 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**. A redireção 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**, a redireção 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, essa configuração é Proibida.

Configurações da política de Lista de Controle de Acesso (ACL) de redirecionamento de conteúdo do navegador

Use essa configuração para configurar uma Lista de Controle de Acesso (ACL) de URLs que podem usar a redireção de conteúdo do navegador ou que têm o acesso negado à redireção 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.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Não permitido: `http://*.xyz.com/`

Você pode obter uma granularidade melhor especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, apenas a página index.html será redirecionada.

Por padrão, esta configuração é definida como `https://www.youtube.com/*`

Para obter mais informações, consulte o artigo do Knowledge Center CTX238236.

Sites de autenticação de redirecionamento de conteúdo do navegador

Use esta configuração para configurar uma lista de URLs. Sites redirecionados usando o redirecionamento de conteúdo do navegador usam a lista para autenticar um usuário. A configuração especifica as URLs para as quais o redirecionamento de conteúdo do navegador permanece ativo (redirecionado) ao navegar para fora de uma URL na lista de permissões.

Um cenário clássico é um site que depende de um Provedor de Identidade (IdP) para autenticação. Por exemplo, um site `www.xyz.com` deve ser redirecionado para o endpoint, mas um IdP de terceiros, como Okta (`www.xyz.okta.com`), lida com a parte da autenticação. O administrador usa a política de configuração de ACL de redirecionamento de conteúdo do navegador para adicionar `www.xyz.com` à lista de permissões. Em seguida, usa os sites de autenticação de redirecionamento de conteúdo do navegador para adicionar `www.xyz.okta.com` à lista de permissões.

Para obter mais informações, consulte o artigo do Knowledge Center CTX238236.

Configuração da lista de bloqueio de redirecionamento de conteúdo do navegador

Esta configuração funciona em conjunto com a configuração de ACL de redirecionamento de conteúdo do navegador. Considere que as URLs estão presentes na configuração de ACL de redirecionamento de conteúdo do navegador e na configuração da lista de bloqueio. Neste caso, a configuração da lista de bloqueio tem precedência e o conteúdo do navegador da URL não é redirecionado.

URLs não autorizadas: Especifica as URLs na lista de bloqueio cujo conteúdo do navegador não é redirecionado para o cliente, mas renderizado no servidor.

O curinga * é permitido, mas não é permitido dentro do protocolo ou da parte do endereço de domínio da URL.

Permitido: `http://www.xyz.com/index.html` , `https://www.xyz.com/*` , `http://www.xyz.com/*videos*`

Não permitido: `http://*.xyz.com/`

Você pode obter uma granularidade melhor especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html` , apenas index.html estará na lista de bloqueio.

Configuração de proxy de redirecionamento de conteúdo do navegador

Esta configuração fornece opções de configuração para as configurações de proxy no VDA para redirecionamento de conteúdo do navegador. Se ativado com um endereço de proxy e número de porta válidos, URL PAC / WPAD ou configuração Direta/Transparente, o aplicativo Citrix Workspace tenta apenas a busca no servidor e a renderização no cliente.

Se desativado ou não configurado e usando um valor padrão, o aplicativo Citrix Workspace tenta a busca e a renderização do 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.

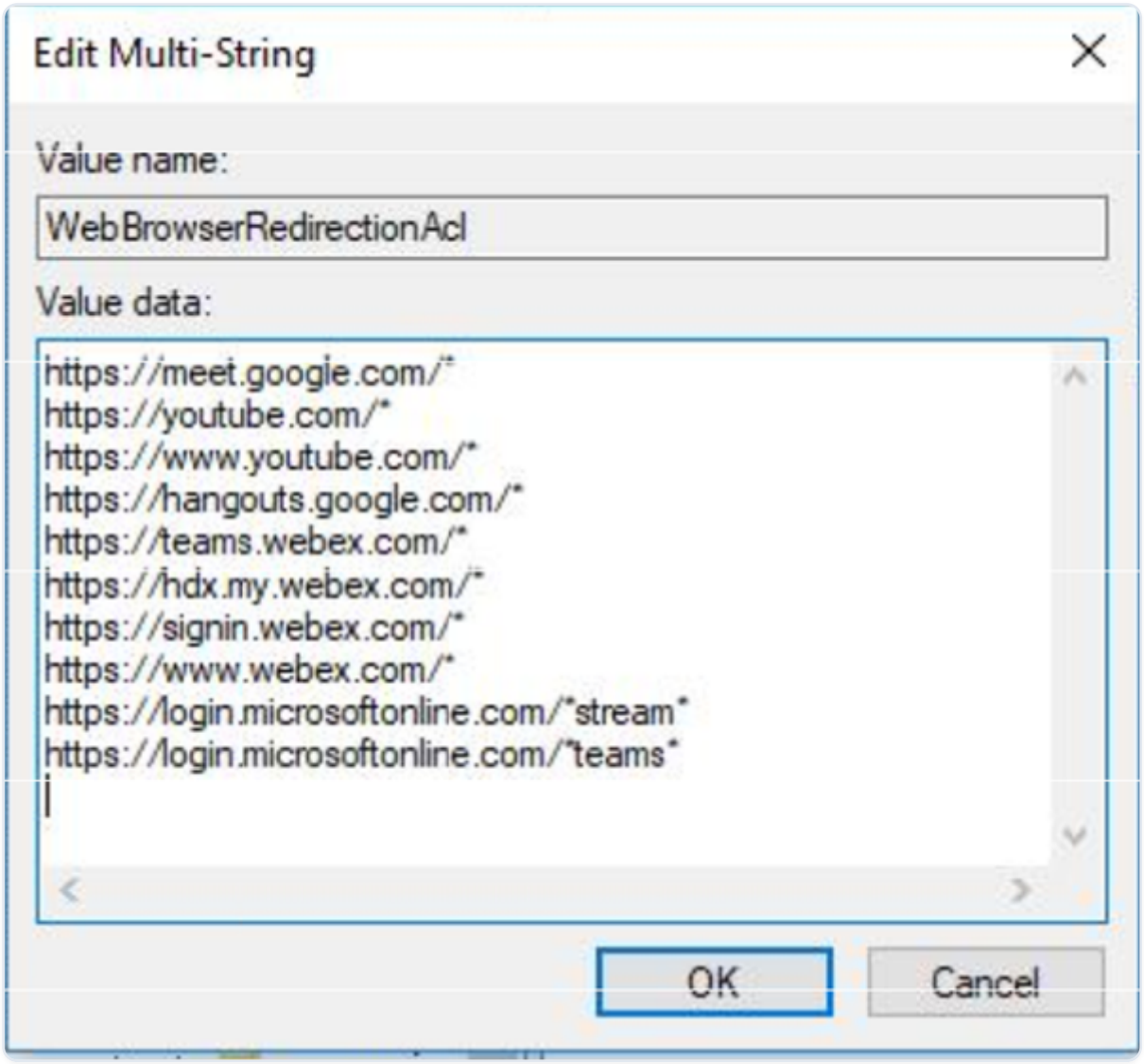
Substituições de chave de registro de redirecionamento de conteúdo do navegador

> **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.

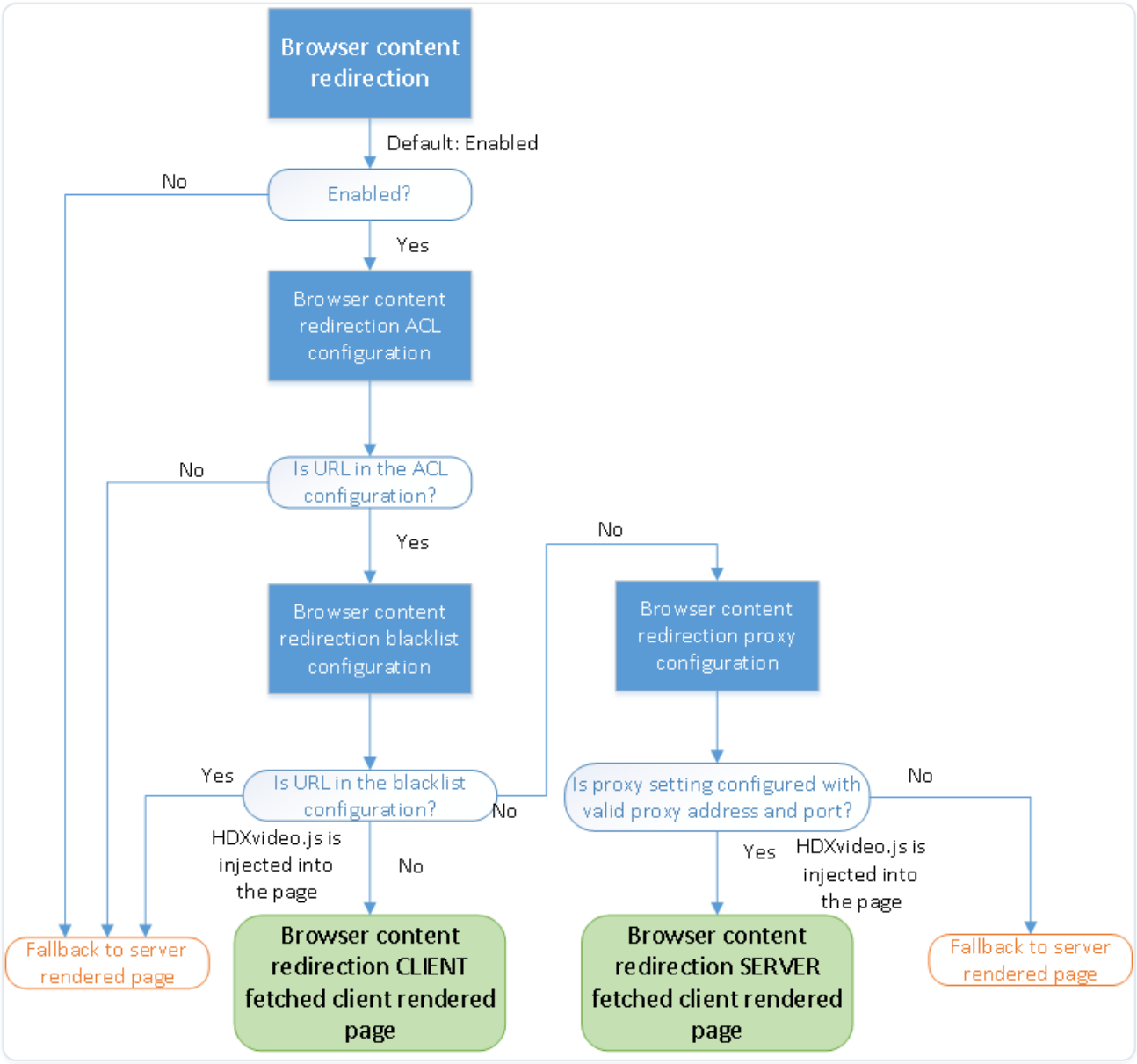
> As entradas de registro substituem as opções para as configurações de política:

`\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`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	


Edit Multi-String
Value name:
WebBrowserRedirectionAcl
Value data:
https://meet.google.com/*
https://youtube.com/*
https://www.youtube.com/*
https://hangouts.google.com/*
https://teams.webex.com/*
https://hdx.my.webex.com/*
https://signin.webex.com/*
https://www.webex.com/*
https://login.microsoftonline.com/*stream*
https://login.microsoftonline.com/*teams*
OK
Cancel

Inserção de HDXVideo.js para redirecionamento de conteúdo do navegador



HdxVideo.js é injetado na página da web usando a extensão do Chrome de redirecionamento de conteúdo do navegador ou o Objeto Auxiliar do Navegador (BHO) do Internet Explorer. O BHO é um modelo de plug-in para o Internet Explorer. Ele fornece ganchos para APIs do navegador e permite que o plug-in acesse o Modelo de Objeto de Documento (DOM) da página para controlar a navegação.

O BHO decide se injeta HdxVideo.js em uma determinada página. A decisão é baseada nas políticas administrativas mostradas no fluxograma anterior.

Depois que ele decide injetar o JavaScript e redirecionar o conteúdo do navegador para o cliente, a página da web fica em branco no navegador Internet Explorer no VDA. Definir **document.body.innerHTML** como vazio remove todo o corpo da página da web no VDA. A página está pronta para ser enviada ao cliente para ser exibida no navegador de sobreposição (Hdxbrowser.exe) no cliente.

Configurações de política de sensores do cliente

A seção **Sensores do Cliente** inclui configurações de política para controlar como as informações do sensor do dispositivo móvel são tratadas em uma sessão de usuário.

Permitir que aplicativos usem a localização física do dispositivo cliente

Essa 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 essa configuração é proibida, as tentativas de um aplicativo de recuperar informações de localização retornam um valor de "permissão negada".

Quando essa 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 permissão na primeira vez que as informações de localização são solicitadas em cada sessão.

Ao desenvolver aplicativos hospedados que usam a configuração Permitir que aplicativos usem a localização física do dispositivo cliente, considere o seguinte:

- Certifique-se de que um aplicativo habilitado para localização não dependa da disponibilidade de informações de localização porque:
  - Um usuário pode não permitir o acesso às informações de localização.
  - A localização pode não estar disponível ou pode mudar enquanto o aplicativo está em execução.
  - Um usuário pode se conectar à sessão do aplicativo a partir de um dispositivo diferente que não oferece suporte a informações de localização.
- Um aplicativo habilitado para localização deve:
  - Ter o recurso de localização desativado por padrão.
  - Fornecer ao usuário uma opção para permitir ou desativar o recurso enquanto o aplicativo está em execução.
  - Forneça ao usuário uma opção para limpar os dados de localização que o aplicativo armazena em cache. (O aplicativo Citrix Workspace não armazena dados de localização em cache.)

- Um aplicativo habilitado para localização deve gerenciar a granularidade das informações de localização. Esse gerenciamento garante que os dados adquiridos sejam apropriados para a finalidade do aplicativo. Além disso, está em conformidade com os regulamentos em todas as jurisdições relevantes.
- Imponha uma conexão segura (por exemplo, usando TLS ou uma VPN) ao usar serviços de localização. Conecte o aplicativo Citrix Workspace a servidores confiáveis.
- Considere obter aconselhamento jurídico sobre o uso de serviços de localização.

Configurações de política de UI do Desktop

A seção **Interface do Usuário da Área de Trabalho** inclui configurações de política que controlam efeitos visuais como papel de parede da área de trabalho, animações de menu e imagens de arrastar. Essas configurações de política ajudam a gerenciar a largura de banda usada nas conexões do 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 o **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 certifique-se de 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.

Configuração da política de experiência de desktop aprimorada

A configuração da política de experiência de desktop aprimorada executa sessões em sistemas operacionais de servidor que se parecem com desktops locais do Windows 7.

Por padrão, esta configuração é permitida.

Se um perfil de usuário com o tema Clássico do Windows existir no desktop virtual, esta política não fornecerá uma experiência de desktop aprimorada para esse usuário. Considere um usuário com um perfil de usuário com tema do Windows 7 que faz logon em um desktop virtual executando o Windows Server 2012. Além disso, esta política não está configurada ou está desabilitada. Neste 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 um desktop virtual com sessões de usuário ativas, a interface dessas sessões se tornará inconsistente em desktops Windows 7 e Windows Clássico. Para evitar essa inconsistência, certifique-se de reiniciar o desktop virtual após alterar esta configuração de política. Em seguida, exclua quaisquer perfis móveis no desktop virtual. A Citrix® também recomenda excluir quaisquer outros perfis de usuário no desktop virtual para evitar inconsistências entre os perfis.

Considere que você está usando perfis de usuário móveis em seu ambiente. Neste caso, certifique-se de que o recurso Experiência de Desktop Aprimorada esteja habilitado ou desabilitado para todos os desktops virtuais que compartilham um perfil.

A Citrix não recomenda compartilhar perfis móveis entre desktops virtuais que executam sistemas operacionais de servidor e sistemas operacionais de cliente. Os perfis para sistemas operacionais de cliente e servidor são diferentes. O compartilhamento de perfis móveis entre ambos os tipos pode levar a inconsistências nas propriedades do perfil quando um usuário se move entre os dois.

Configurações de política de Redirecionamento de Arquivos

A seção **Redirecionamento de Arquivos** inclui configurações de política relacionadas ao mapeamento de unidades cliente e à otimização de unidades cliente.

Conectar automaticamente unidades cliente

Essa configuração permite ou impede a conexão automática de unidades cliente quando os usuários fazem logon.

Por padrão, a conexão automática é permitida.

Ao adicionar essa 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 essa 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

Essa 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 da 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. Essa 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 essa 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 de cliente automaticamente**.

Unidades de rede do cliente

Esta configuração permite ou impede que os usuários acessem e salvem arquivos em unidades de rede (remotas) por meio 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. Essa configuração é aplicável independentemente do estado da configuração **Unidades de rede do cliente**.

Para garantir que as unidades de rede sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades de cliente automaticamente**.

Unidades ópticas do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos nos seguintes locais:

- CD-ROM no dispositivo do usuário
- DVD-ROM no dispositivo do usuário
- Unidades BD-ROM no dispositivo do usuário.

Por padrão, o acesso a unidades ópticas do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja presente e definida como **Permitido**. Se essas configurações estiverem desabilitadas, as unidades ópticas do cliente não serão mapeadas e os

usuários não poderão acessá-las manualmente. 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 automaticamente unidades cliente**.

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 automaticamente unidades cliente** para garantir que as unidades removíveis sejam conectadas automaticamente quando os usuários fizerem logon.

Redirecionamento do host para o cliente

Esta configuração habilita ou desabilita associações de tipo de arquivo para URLs e alguns conteúdos de mídia a serem abertos no dispositivo do usuário. Quando desabilitado, o conteúdo é aberto no servidor.

Por padrão, a associação de tipo de arquivo está desabilitada.

Esses tipos de URL são abertos localmente quando você habilita esta configuração:

- HTTP
- HTTPS
- Real Player e QuickTime (RTSP)
- Real Player e QuickTime (RTSPU)
- Real Player Legado (PNM)
- Microsoft Media Server (MMS)

Preservar letras de unidade do cliente

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 definida 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 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 aplicativo Citrix Workspace 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 este 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 que o redirecionamento de pasta especial funcione. Essa situação ocorre porque o redirecionamento de pasta especial deve interagir com o dispositivo do usuário.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Unidades fixas do cliente** esteja presente e definida como Permitido.

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 desabilitada, 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 compactação visualmente sem perdas

Essa configuração permite que a compactação visualmente sem perdas seja usada em vez da compactação verdadeiramente sem perdas para gráficos. A compactação visualmente sem perdas melhora o desempenho em relação à verdadeiramente sem perdas, mas tem uma perda menor que é imperceptível à vista. Essa configuração altera a forma como os valores da configuração Qualidade visual são usados.

Por padrão, essa configuração está desabilitada.

Indicador de status gráfico

Essa configuração configura o indicador de status gráfico para ser executado na sessão do usuário. Essa ferramenta permite que o usuário veja informações sobre o modo gráfico ativo. As

informações incluem detalhes sobre codec de vídeo, codificação de hardware, qualidade da imagem e monitores em uso para a sessão. Com o indicador de status gráfico, o usuário também pode habilitar ou desabilitar o modo pixel-perfect.

As versões do Citrix Virtual Apps and Desktops™ 2103 e posteriores incluem um controle deslizante de qualidade de imagem para ajudar o usuário a encontrar o equilíbrio certo entre qualidade de imagem e interatividade.

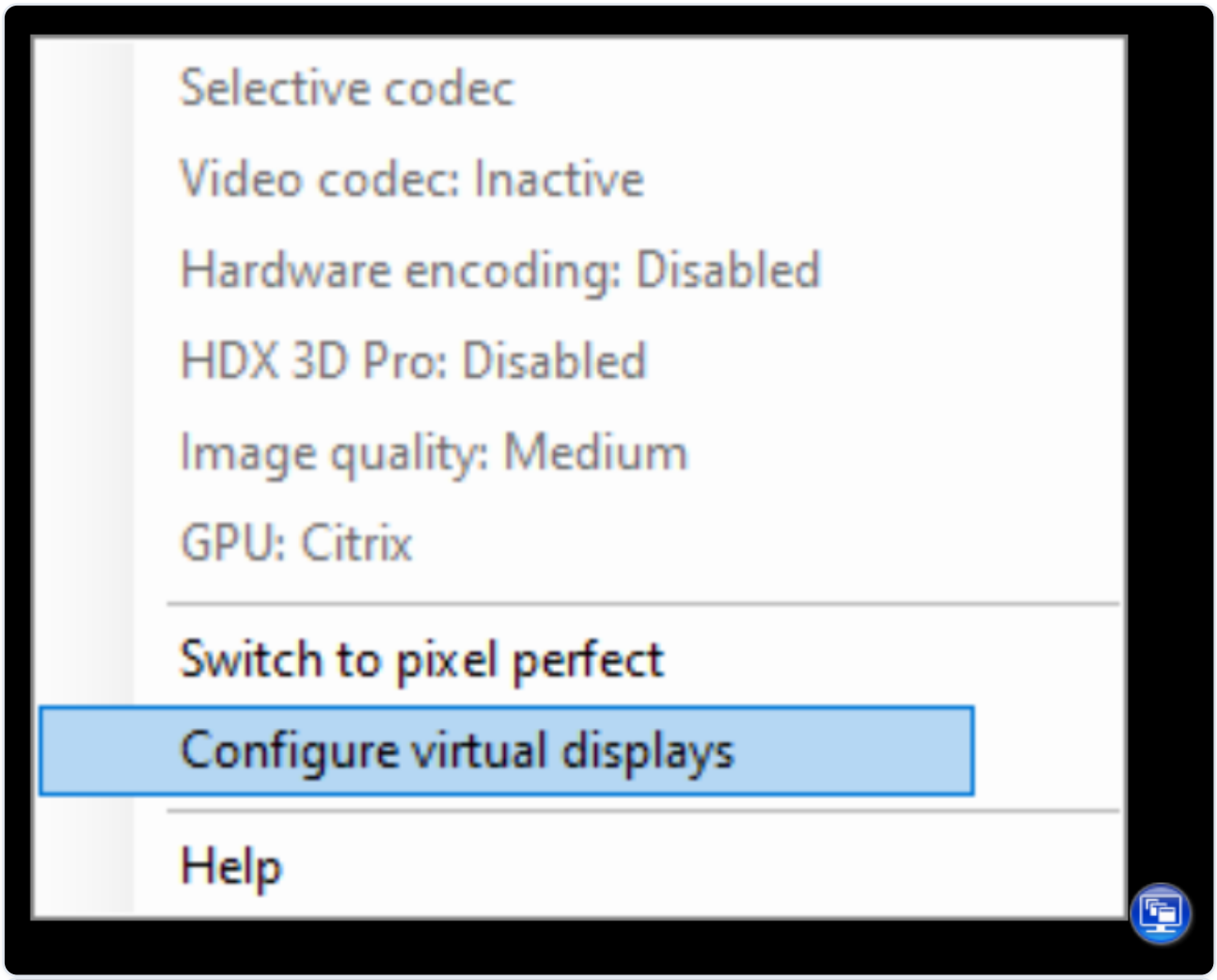
As versões do Citrix Virtual Apps and Desktops 2109 e posteriores incluem funcionalidade para configurar um layout de exibição virtual por meio de uma interface de usuário iniciada usando o indicador de status gráfico.

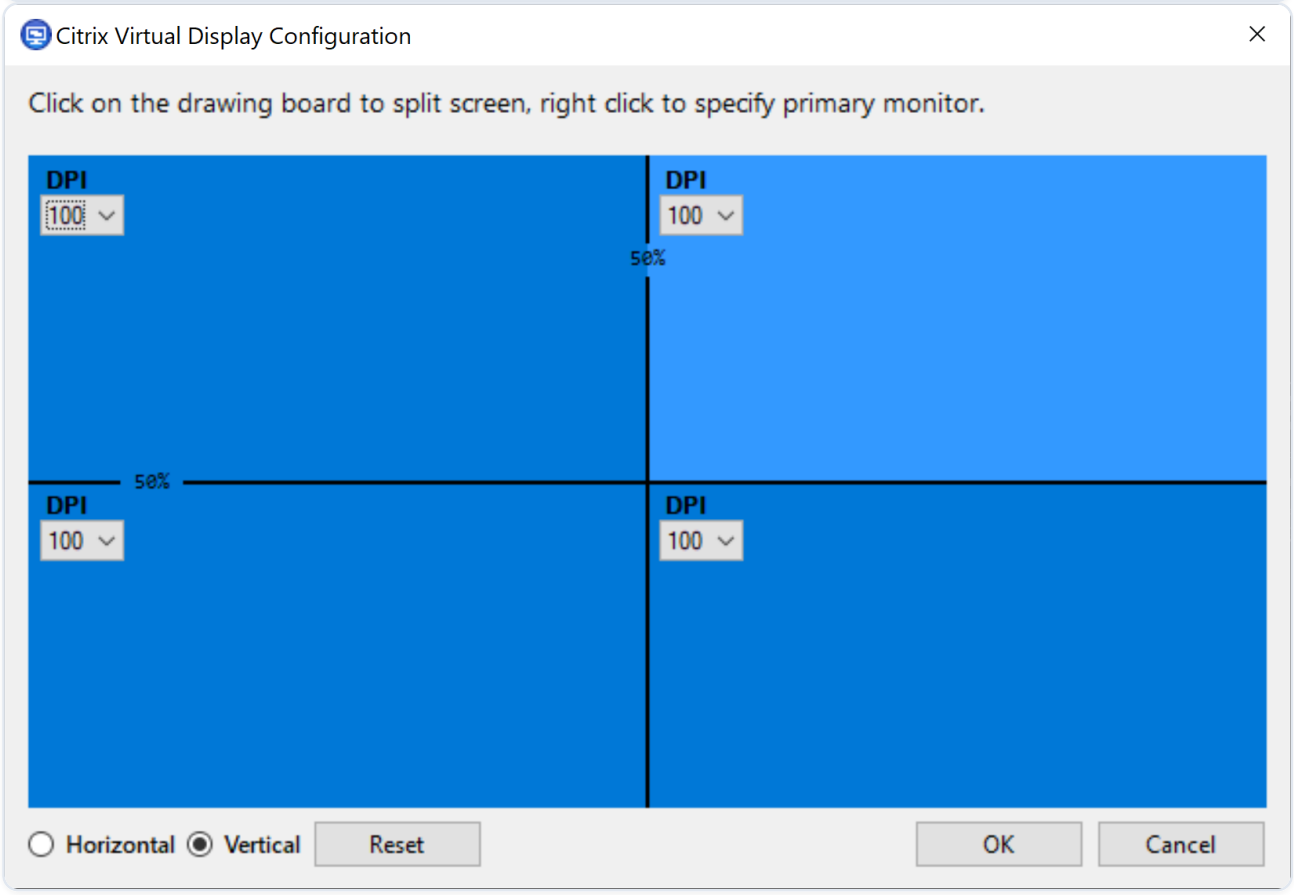
O indicador de status gráfico substitui a ferramenta de indicador sem perdas de versões anteriores. Essa política habilita o indicador sem perdas para as versões 7.16 a 1809 do Citrix Virtual Apps and Desktops.

Layout de exibição virtual

O recurso de layout de exibição virtual, já parte do Citrix Workspace™ app para Windows, agora também faz parte do VDA. Esse recurso permite definir um layout de monitor virtual no VDA dentro de uma sessão ativa e dividir virtualmente os monitores da sessão em até oito exibições virtuais na área de trabalho remota. Você pode configurar os monitores virtuais clicando com o botão direito do mouse no ícone do indicador de status gráfico e selecionando a opção **Configurar exibições virtuais**, que inicia a interface do usuário de configuração de exibição virtual. Lá, você pode desenhar linhas horizontais ou verticais para separar a tela em monitores virtuais. Clicar com o botão direito do mouse em um monitor virtual na interface do usuário o marca como monitor principal. A tela é dividida de acordo com porcentagens especificadas das resoluções do monitor da sessão. Você também pode definir um DPI para as exibições virtuais.

Depois de definir um layout de monitor virtual, clicar em **OK** aplica imediatamente o layout de exibição virtual. **Cancelar** fecha a interface do usuário, descartando quaisquer alterações.


Selective codec
Video codec: Inactive
Hardware encoding: Disabled
HDX 3D Pro: Disabled
Image quality: Medium
GPU: Citrix
Switch to pixel perfect
Configure virtual displays
Help


Citrix Virtual Display Configuration
Click on the drawing board to split screen, right click to specify primary monitor.
DPI
100
DPI
100
50%
50%
DPI
100
DPI
100
Horizontal
Vertical
Reset
OK
Cancel

Esta configuração se aplica apenas a sessões de desktop e não afeta nenhum aplicativo publicado. Em um cenário de vários monitores, o mesmo layout de exibição virtual configurado é aplicado a todos os monitores da sessão, se o número total de exibições virtuais não exceder o máximo suportado de oito exibições virtuais. Caso esse limite seja excedido, o layout de exibição virtual é ignorado e não é aplicado a nenhum monitor de sessão.

A configuração de exibição virtual definida 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 em redimensionamento de sessão, desconexão/reconexão de sessão e logoff/logon de sessão.

Não use este recurso simultaneamente com o recurso de exibição virtual existente no Citrix Workspace App.

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 de modo gráfico herdado estiver ativada.

O HDX™ aloca apenas a quantidade de memória de vídeo 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 vídeo.

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 de modo gráfico herdado está ativada.

> Quando o limite de memória de vídeo da sessão é atingido, esta configuração especifica se a profundidade de cor ou a resolução degrada primeiro.

Por padrão, a profundidade de cor é degradada primeiro.

Quando o limite de memória da sessão é atingido, você pode reduzir a qualidade das imagens exibidas. Você pode reduzir essa qualidade escolhendo se a profundidade de cor ou a resolução é degradada primeiro. Quando a profundidade de cor é degradada primeiro, as imagens exibidas usam menos cores. Quando a resolução é degradada primeiro, as imagens exibidas usam menos pixels por polegada.

Para notificar os usuários quando a profundidade de cor ou a resolução for degradada, configure a configuração Notificar usuário quando o modo de exibição for degradado.

Visualização dinâmica de janelas

Esta configuração ativa ou desativa a exibição de janelas contínuas em:

- Flip-
- Flip 3D
- Visualização da barra de tarefas
- Espiar janelas

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.
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 pela tela.

Por padrão, esta configuração está ativada.

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 ativada.

> Esta configuração ativa ou desativa o cache e a recuperação de seções de imagens em sessões. O cache de imagens em seções e a recuperação dessas seções quando necessário torna 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 do modo gráfico herdado estiver ativada.

Modo gráfico herdado - não suportado. Apenas para compatibilidade com versões anteriores

> **Importante:**
>
> Não oferecemos suporte ao modo gráfico herdado e à Redireção de Composição da Área de Trabalho (DCR) nesta versão. Esta política está 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 desativa a experiência gráfica rica. Use esta configuração para reverter para a experiência gráfica herdada, reduzindo o consumo de largura de banda em uma WAN ou conexão móvel. As reduções de largura de banda introduzidas no XenApp e XenDesktop 7.13 tornam este modo obsoleto.

Por padrão, esta configuração está desativada e os usuários recebem a experiência gráfica rica.

O modo gráfico herdado é suportado nos seguintes:

- Windows 7
- VDAs do Windows Server 2008 R2.

O modo gráfico herdado não é suportado nos seguintes:

- 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 máxima de cor permitida

> **Observação:**

> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política do modo gráfico herdado está ativada.

> 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 vídeo principal. Esses VDAs são VDAs que usam um driver Windows Display Driver Model (WDDM) como driver de vídeo principal. Para VDAs de SO de sessão única que usam um driver WDDM como driver de vídeo principal, como o Windows 8, essa configuração não tem efeito. Para VDAs de SO de várias sessões 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 do 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 desativada.

Otimizar para carga de trabalho de gráficos 3D

Essa configuração configura as definições 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 esta 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 do modo gráfico herdado está habilitada.

> Essa configuração descarta imagens enfileiradas que são substituídas por outra imagem.

Por padrão, o enfileiramento e descarte está ativado.

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 irregulares 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 alteração ativa** é selecionado, o codec de vídeo é usado para áreas onde há mudança constante na tela, outros dados usam compactação de imagem estática e cache de bitmap. Quando a decodificação de vídeo não está disponível no endpoint, ou quando você especifica **Não usar codec de vídeo**, uma combinação de compactação de imagem estática e cache de bitmap é usada. Quando **Usar quando**

preferencial é selecionado, o sistema escolhe, com base em vários fatores. Os resultados podem variar entre as versões à medida que o método de seleção é aprimorado.

Selecione **Usar quando preferencial** para permitir que o sistema faça o seu melhor para escolher as configurações apropriadas para o cenário atual.

Selecione **Para a tela inteira** para otimizar a experiência do usuário e a largura de banda, especialmente em casos de uso intenso de vídeo renderizado por servidor e gráficos 3D.

Selecione **Para regiões em alteração ativa** para otimizar o desempenho de vídeo, especialmente em baixa largura de banda, mantendo a escalabilidade para conteúdo estático e em mudança lenta. Essa configuração é suportada em implantações de 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

Essa 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 essa configuração de política é **Habilitado**.

Vários monitores são suportados.

Qualquer aplicativo Citrix Workspace que suporte decodificação de vídeo pode ser usado com codificação de hardware.

NVIDIA

Para GPUs NVIDIA GRID, a codificação de hardware é suportada com VDAs para Multi-session OS e Single-session OS.

As GPUs NVIDIA devem suportar a codificação de hardware NVENC. Consulte NVIDIA video codec SDK para obter uma lista de GPUs suportadas.

O NVIDIA GRID requer a versão de driver 3.1 ou superior. O 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. A compressão visualmente sem perdas (configuração de política gráfica, Permitir compressão visualmente sem perdas) requer o Citrix Workspace app 1808 ou superior ou o Citrix Receiver para Windows 4.5 ou superior.

INTEL

Para processadores gráficos Intel Iris Pro, a codificação de hardware é suportada com VDAs para SO de sessão única e SO de múltiplas sessões.

Os processadores gráficos Intel Iris Pro da família de processadores Intel Broadwell e posteriores são suportados. É necessária a versão 1.0 do Intel Remote Displays SDK, que pode ser baixada do site da Intel: Remote Displays SDK.

O texto sem perdas é suportado apenas quando a política de codec de vídeo está definida para a tela inteira e a política **Otimizar para carga de trabalho de gráficos 3D** está desativada.

Visualmente sem perdas (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 forem necessárias mais de oito sessões de codificação, verifique quantos monitores a máquina virtual conecta. O administrador decide configurar essa configuração de 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 RapidFire SDK. Por exemplo, as GPUs AMD Radeon Pro ou FirePro.

Para que a codificação funcione, instale os drivers AMD mais recentes. Você pode baixar esses drivers em `<https://www.amd.com/en/support>`.

O texto sem perdas não é compatível com a codificação de hardware AMD. Se você ativou o texto sem perdas, o texto sem perdas tem prioridade sobre a codificação de hardware AMD.

O uso seletivo do codec de hardware H.264 para regiões em mudança ativa é suportado.

Configurações de política de cache

Esta seção inclui configurações de política que permitem o cache de dados de imagem em dispositivos de usuário quando as conexões do cliente são limitadas em largura de banda.

LIMITE DE CACHE PERSISTENTE

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 habilitada.

Esta configuração armazena bitmaps em cache no disco rígido do dispositivo do usuário e, assim, permite a reutilização de imagens grandes e frequentemente usadas de sessões anteriores.

Por padrão, o limite é de 3.000.000 bits por segundo.

O valor do limite representa o ponto abaixo do qual o recurso de Cache Persistente entra em vigor. Por exemplo, usando o valor padrão, os bitmaps são armazenados em cache no disco rígido do dispositivo do usuário quando a largura de banda cai abaixo de 3.000.000 bps.

Configurações de política do Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais suportado. Em vez disso, use Thinwire com transporte adaptável ativado.

> A seção **Framehawk** inclui configurações de política que ativam e configuram o canal de exibição Framehawk no servidor.

CANAL DE EXIBIÇÃO FRAMEHAWK

Quando ativado, o servidor tenta usar o canal de exibição Framehawk para os gráficos do usuário e o acesso remoto de entrada. Esse canal de exibição usa UDP para fornecer uma melhor experiência do usuário em redes com alta perda e características de latência. No entanto, ele também pode usar mais recursos do servidor e largura de banda do que outros modos gráficos.

Por padrão, o canal de exibição Framehawk está desativado.

INTERVALO DE PORTAS DO CANAL DE EXIBIÇÃO FRAMEHAWK

Essa configuração de política especifica o intervalo de números de porta UDP que o VDA usa para trocar dados do canal de exibição Framehawk com o dispositivo do usuário. Os números de porta estão no formato *número de porta mais baixo ou número de porta mais alto*. O VDA tenta usar cada porta, começando com o número de porta mais baixo e incrementando a cada tentativa subsequente. A porta lida com o tráfego de entrada e saída.

Por padrão, o intervalo de portas é 3224,3324.

Configurações de política de keep-alive

A seção **Keep Alive** contém configurações de política para gerenciar mensagens keep-alive do ICA®.

Tempo limite de keep-alive do ICA

Essa configuração especifica o número de segundos entre mensagens keep-alive ICA 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 keep-alive ICA. Não configure essa definição se o seu software de monitoramento de rede for responsável por fechar conexões inativas.

Mensagens keep-alive do ICA

Essa configuração habilita ou desabilita o envio periódico de mensagens keep-alive ICA.

Por padrão, as mensagens keep-alive não são enviadas.

Habilitar essa configuração impede que conexões quebradas sejam desconectadas. Se o servidor não detectar atividade, essa 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 keep-alive do ICA não funciona se você estiver usando a confiabilidade da sessão. Configure o keep-alive do ICA apenas para conexões que não estão usando a Confiabilidade da Sessão.

Configurações de política relacionadas: Conexões de confiabilidade da sessão.

Configurações de política de Acesso a Aplicativos Locais

A seção **Acesso a Aplicativos Locais** inclui configurações de política que gerenciam os aplicativos instalados localmente dos usuários com aplicativos hospedados. Essas configurações de política gerenciam a integração em um ambiente de área de trabalho hospedada.

Permitir Acesso a Aplicativos Locais

Essa configuração permite ou impede a integração de aplicativos instalados localmente dos usuários com aplicativos hospedados. Essas configurações de política gerenciam a integração em um ambiente de área de trabalho hospedada.

Quando um usuário inicia um aplicativo instalado localmente, esse aplicativo parece ser executado em sua área de trabalho virtual, embora esteja realmente sendo executado localmente.

Se você definir a configuração de política **Permitir acesso a aplicativos locais** como **Ativado**, o redirecionamento de conteúdo do navegador não será compatível e o status da bateria da área de notificação do lado do cliente não aparecerá nas sessões da área de trabalho.

Por padrão, o **Acesso a Aplicativos Locais** é proibido.

Lista de bloqueio de redirecionamento de URL

Essa configuração especifica os sites que são redirecionados e iniciados no navegador da Web local. Esses sites podem incluir o seguinte:

- Sites que exigem informações de localidade, como msn.com ou newsgoogle.com
- Ou
- Sites que contêm conteúdo de mídia avançada que são melhor renderizados no dispositivo do usuário.

Por padrão, nenhum site é especificado.

Lista de permissão de redirecionamento de URL

Essa configuração especifica os sites que são renderizados no ambiente em que são iniciados.

Por padrão, nenhum site é especificado.

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:

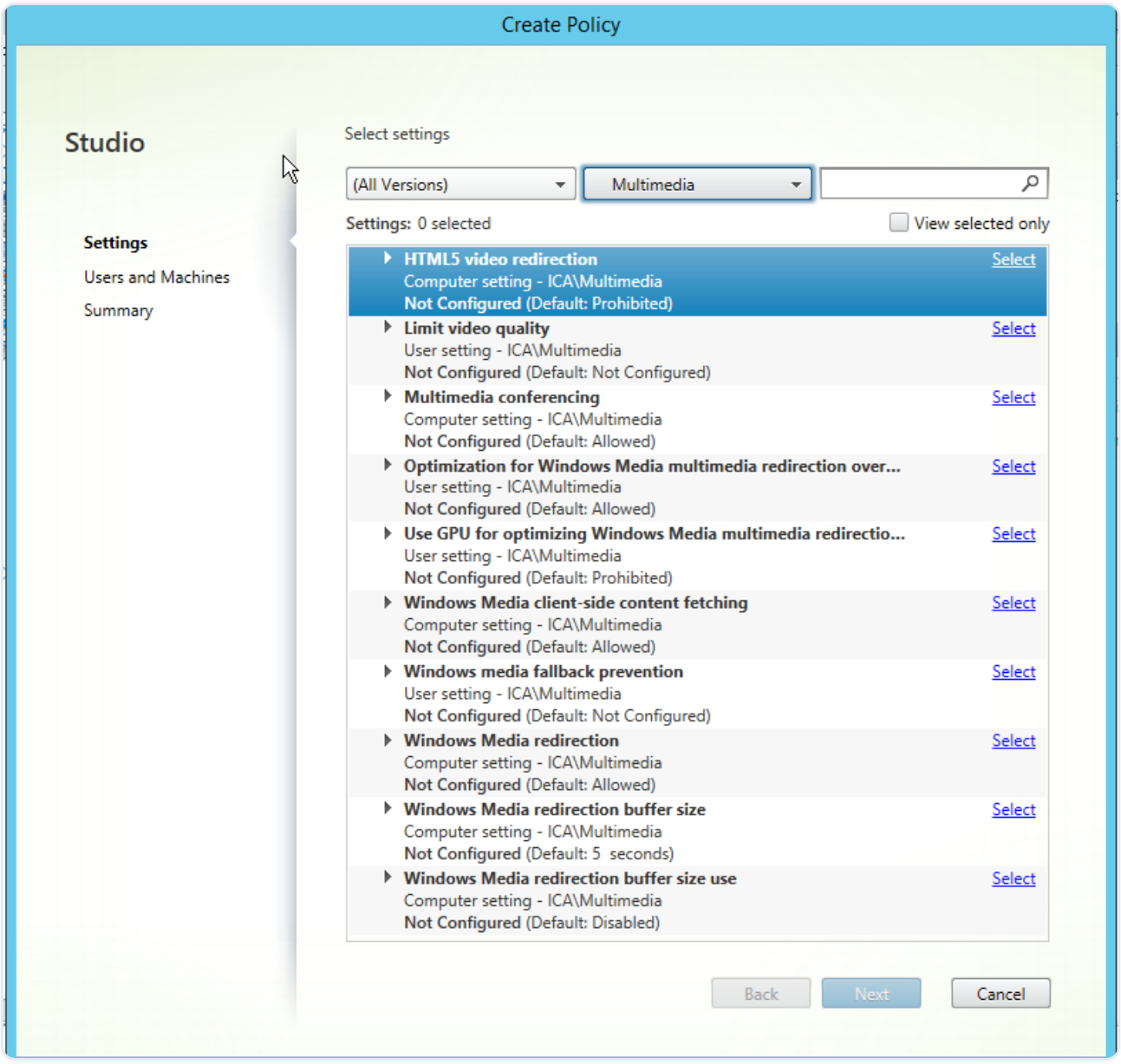
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

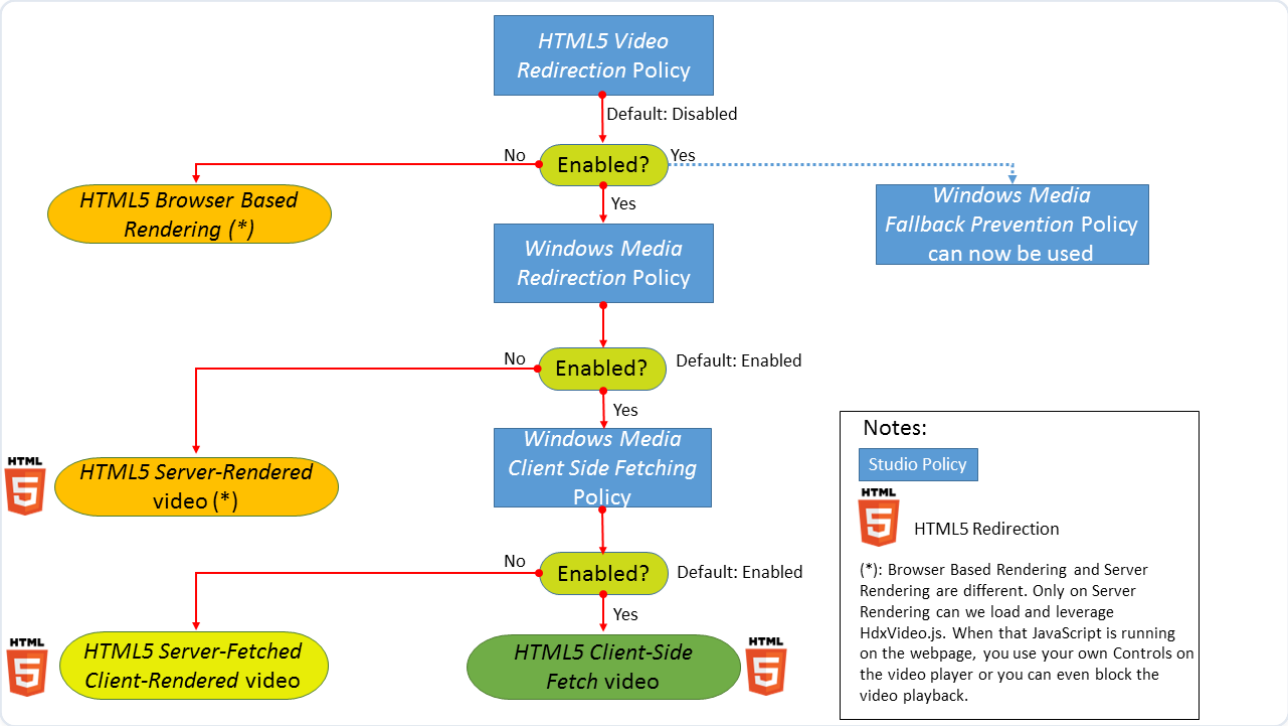
Para localizar o ID da sessão do usuário atual, execute o comando **qwinsta** na linha de comando do Windows.

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. Ele requer a adição de JavaScript às páginas da web onde o conteúdo multimídia HTML5 está disponível, por exemplo, vídeos em um site de treinamento interno.

Para configurar o redirecionamento de vídeo HTML5:

1. Copie o arquivo, **HdxVideo.js**, de %Program Files%/Citrix/ICA Service/HTML5 Video Redirection na instalação do VDA para o local da sua página da web interna.
2. Insira esta linha em sua página da web (se sua página da web tiver outros scripts, inclua **HdxVideo.js** antes desses scripts): `<script src="HdxVideo.js" type="text/javascript"\></script>`

Nota: Se HdxVideo.js não estiver no mesmo local que sua página da web, use o atributo **src** para especificar o caminho completo para ele.

Considere que o JavaScript não foi 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 *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
- pausar
- procurar
- repetir
- áudio
- tela cheia

Você pode visualizar uma página de teste de redirecionamento de vídeo HTML5.

TLS, REDIRECIONAMENTO DE VÍDEO HTML5 E REDIRECIONAMENTO DE CONTEÚDO DO NAVEGADOR

Você pode usar o redirecionamento de vídeo HTML5 para:

- Redirecionar vídeos de sites HTTPS
- Ou
- Redirecionamento de conteúdo do navegador para redirecionar o site inteiro

O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) em execução no VDA. O Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX no armazenamento de certificados no VDA gera dois certificados personalizados para:

- Realizar o redirecionamento de vídeo
- Manter a integridade TLS da página da web

HdxVideo.js usa WebSockets Seguros para se comunicar com o WebSocketService.exe em execução no VDA. Este processo é executado como uma conta de Sistema Local e realiza a terminação SSL e o mapeamento de sessão do usuário.

WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

Limitar a qualidade do vídeo

Esta configuração se aplica apenas ao Windows Media e não ao HTML5. Ela exige que você habilite **Otimização para redirecionamento multimídia do Windows Media sobre WAN**.

Esta configuração especifica o nível máximo de qualidade de vídeo permitido para uma conexão HDX™. Quando configurada, a qualidade máxima 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.

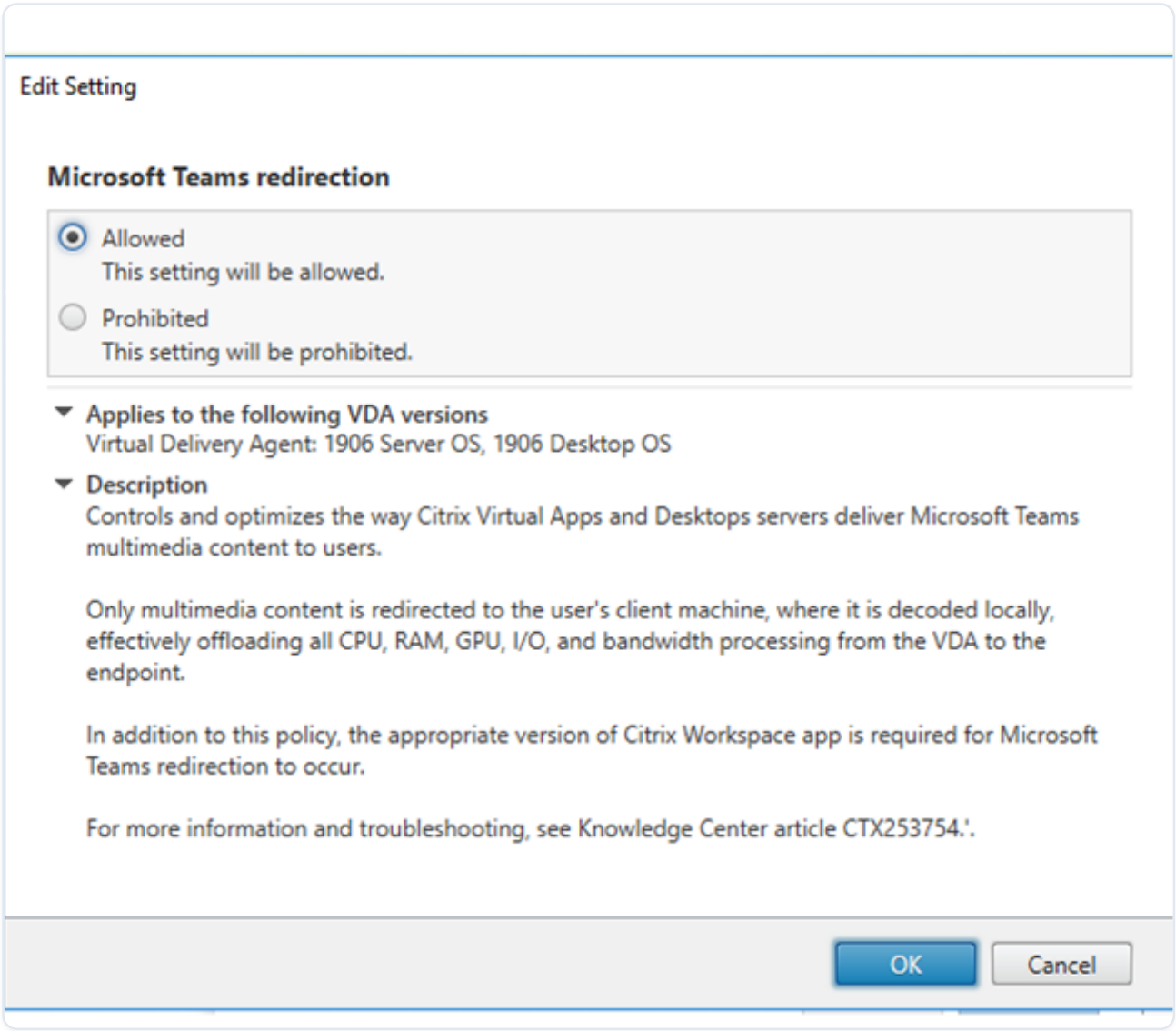
Para limitar o nível máximo de qualidade de vídeo permitido, escolha uma das seguintes opções:

- 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 Studio. Um exemplo de uma versão mais antiga do controller é a versão 7.15. Neste caso, a otimização HDX é ativada

> 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 da Central de Conhecimento CTX205549.

> Neste caso, para desativar 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 ativado.

Conferência multimídia

Esta 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 esta 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.

Esta 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

Esta 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 do Windows Media** esteja presente e definida como **Permitido**.

Quando esta configuração está habilitada, 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 sobre 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 suportada para aceleração de hardware. Caso contrário, a transcodificação retorna para a CPU.

Nota: A transcodificação por GPU é suportada apenas em GPUs NVIDIA.

Por padrão, o uso da GPU no VDA para otimizar a entrega de conteúdo do Windows Media pela WAN é proibido.

Ao adicionar esta configuração a uma política, certifique-se de que as seguintes configurações estejam presentes e definidas como Permitido:

- **Redirecionamento do Windows Media**
- **Configurações de otimização para redirecionamento multimídia do Windows Media sobre WAN**

Prevenção de fallback do Windows Media

Esta configuração se aplica ao redirecionamento de conteúdo do navegador, HTML5 e Windows Media. Para que ele suporte HTML5, defina a política **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.

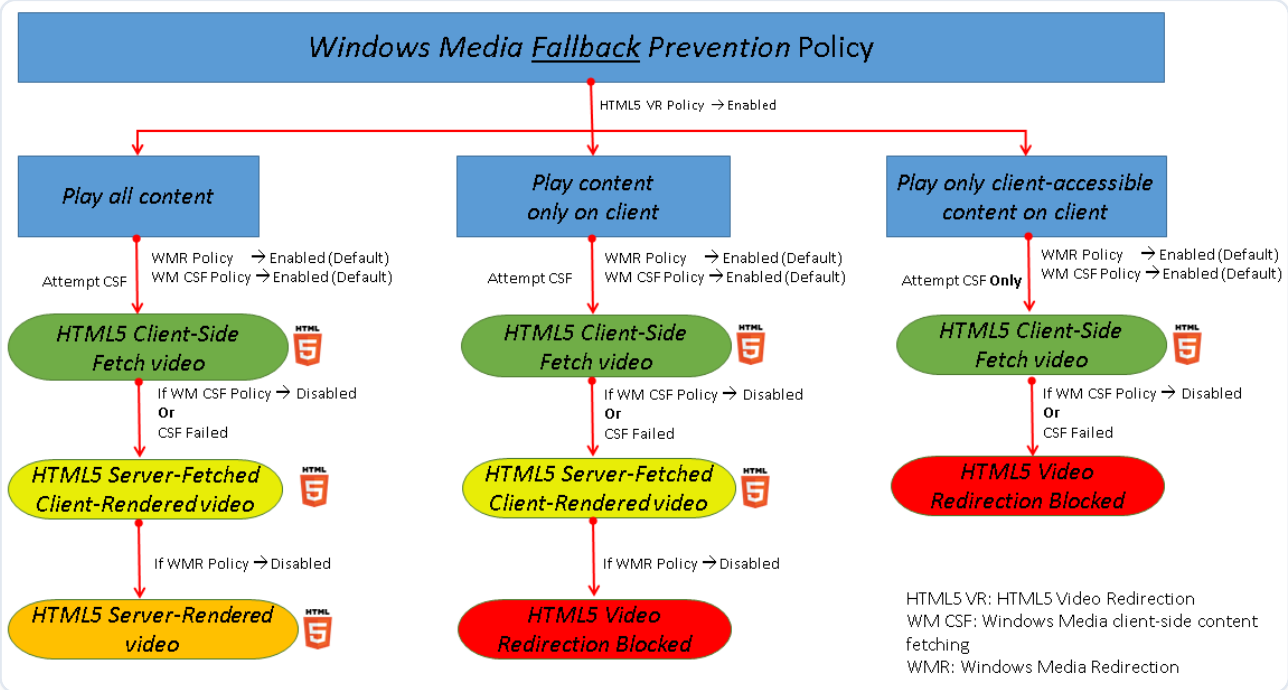
Por padrão, esta configuração não está configurada. Quando a configuração é definida como Não Configurado, o comportamento é o mesmo que **Reproduzir todo o conteúdo**.

Para configurar essa definição, escolha uma das seguintes opções:

- **Reproduzir todo o conteúdo**. Tentar buscar conteúdo no 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 no 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 a busca no 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 dessa 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 DWORD (padrão = 5)

Unidade: segundos

Busca de conteúdo do lado do cliente do Windows Media

Essa configuração se aplica tanto ao HTML5 quanto ao Windows Media. A configuração permite que um dispositivo de usuário transmita arquivos multimídia diretamente do provedor de origem na internet ou intranet, em vez de através do servidor host XenApp ou XenDesktop®.

Por padrão, essa configuração é **Permitida**. Permitir essa configuração melhora o uso da rede e a escalabilidade do servidor. Essa melhoria é alcançada movendo qualquer processamento de mídia do servidor host para o dispositivo do usuário. Também remove a exigência de que uma estrutura multimídia avançada, como Microsoft DirectShow ou Media Foundation, seja instalada no dispositivo do usuário. O dispositivo do usuário requer apenas a capacidade de reproduzir um arquivo de uma URL.

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento do Windows Media** esteja presente e definida como **Permitida**. Se o **Redirecionamento do Windows Media** estiver desabilitado, a transmissão de arquivos multimídia para o dispositivo do usuário diretamente do provedor de origem também será desabilitada.

Redirecionamento do Windows Media

Essa configuração se aplica tanto ao HTML5 quanto ao Windows Media e controla e otimiza a forma como os servidores entregam áudio e vídeo em streaming aos usuários.

Por padrão, essa configuração é **Permitida**. Para HTML5, essa configuração não tem efeito se a política **Redirecionamento de vídeo HTML5** for **Proibida**.

Quando essa configuração está habilitada, a qualidade do áudio e vídeo renderizados do servidor aumenta para um nível comparável ao áudio e vídeo reproduzidos localmente em um dispositivo

de usuário. O servidor transmite multimídia para o cliente na forma original e compactada e permite que o dispositivo do usuário descompacte e renderize a mídia.

O redirecionamento do Windows Media otimiza arquivos multimídia 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 é desabilitado no Citrix Workspace app. Para permitir que os usuários executem aplicativos multimídia em sessões ICA®, ative o áudio ou dê aos usuários permissão para ativar o áudio em sua interface do Citrix Workspace app.

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 acontecer 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 herdada 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

Esta configuração é legada e não se aplica ao HTML5.

Esta configuração habilita ou desabilita o uso do tamanho do buffer especificado na configuração **Tamanho do buffer de redirecionamento do Windows Media**.

Por padrão, o tamanho do buffer especificado não é usado.

Se esta configuração estiver desabilitada ou se a configuração **Tamanho do buffer de redirecionamento do Windows Media** não estiver configurada, o servidor usará o valor padrão do tamanho do buffer (cinco segundos).

Configurações de política de conexões multi-stream

A seção **Conexões Multi-Stream** inclui configurações de política para gerenciar a priorização da 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 ativada.

Áudio sobre UDP

Esta configuração permite ou impede áudio sobre UDP no servidor.

Por padrão, o áudio sobre UDP é permitido no servidor.

Quando ativada, 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, esse intervalo é definido como 16500,16509.

Política Multi-Porta

Essa configuração especifica as portas TCP a serem usadas para o tráfego ICA e estabelece a prioridade de rede para cada porta.

Por padrão, a porta primária (2598) tem prioridade Alta.

Ao configurar portas, você pode atribuir as seguintes prioridades:

- **Muito Alta:** para atividades em tempo real, como conferências por webcam
- **Alta:** para elementos interativos, como tela, teclado e mouse
- **Média:** para processos em massa, como mapeamento de unidade de cliente
- **Baixa:** para atividades em segundo plano, como impressão

Cada porta deve ter uma prioridade exclusiva. Por exemplo, você não pode atribuir uma prioridade Muito Alta às portas CGP 1 e CGP 3.

Para remover uma porta da priorização, defina o número da porta como 0. Você não pode remover a porta primária e não pode alterar seu nível de prioridade.

Ao configurar esta definição, reinicie o servidor. Esta definição só entra em vigor quando a definição de política **Multi-Stream computer** está ativada.

Definição de computador Multi-Stream

Esta definição ativa ou desativa o Multi-Stream no servidor.

Por padrão, o Multi-Stream está desativado. Configure a definição de política de computador Multi-Stream se você usar Citrix SD-WAN™ ou roteadores de terceiros para obter a Qualidade de Serviço desejada.

Se o Multi-Stream estiver ativado, 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 limite de largura de banda geral 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 sejam incluídas.

Configurações de atribuição de canal virtual Multi-Stream

Esta configuração especifica o fluxo ICA ao qual os canais virtuais são atribuídos quando o multi-stream é usado.

Se você não configurar essas configurações, os canais virtuais serão mantidos em seu fluxo padrão. Para atribuir um canal virtual a um fluxo ICA, selecione o número do fluxo desejado (0, 1, 2, 3) na lista **Número do Fluxo** ao lado do nome do canal virtual.

Se houver um canal virtual personalizado em uso no ambiente, clique em **Adicionar**, especifique o nome do canal virtual na caixa de texto em **Canais Virtuais** e selecione o número do fluxo desejado na lista **Número do Fluxo** ao lado dele. O nome que você especificar deve ser o nome real do canal virtual e não um nome amigável. Por exemplo, CTXSBR em vez de Citrix Browser Acceleration.

Essas configurações só 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 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 de Microsoft Teams/WebRTC: 1
- Receiver Móvel: 1
- MultiToque: 1
- Encaminhamento de Porta: 2
- Extensões de Áudio e Vídeo Remoto (RAVE): 2
- Seamless (Integração de Janela Transparente): 1
- Sensor e Localização: 1
- Cartão Inteligente: 1
- Thinwire Graphics: 1
- Integração de UI Transparente/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 da Central de Conhecimento CTX131001.

Configurações de política de redirecionamento de porta

A seção **Redirecionamento de Porta** contém configurações de política para mapeamento de porta LPT e COM do cliente.

Para versões do Virtual Delivery Agent **anteriores a 7.0**, use as seguintes configurações de política para configurar o redirecionamento de porta. Para as versões do VDA **7.0 a 7.8**, configure

essas configurações usando o registro; consulte Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro. Para a versão do VDA **7.9**, use as seguintes configurações de política.

Conectar automaticamente portas COM do cliente

Essa configuração habilita ou desabilita a conexão automática de portas COM em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas COM do cliente não são conectadas automaticamente.

Conectar automaticamente portas LPT do cliente

Essa configuração habilita ou desabilita a conexão automática de portas LPT em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas LPT do cliente não são conectadas automaticamente.

Redirecionamento de porta COM do cliente

Essa configuração permite ou impede o acesso a portas COM no dispositivo do usuário.

Por padrão, o redirecionamento de porta COM é proibido.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta COM
- Porcentagem de limite de largura de banda de redirecionamento de porta COM

Redirecionamento de porta LPT do cliente

Esta configuração permite ou impede o acesso às portas LPT no dispositivo do usuário.

Por padrão, o redirecionamento de porta LPT é proibido.

As portas LPT são usadas apenas por aplicativos legados que enviam trabalhos de impressão para as portas LPT. Essas portas não são usadas por aplicativos legados que enviam trabalhos de impressão para os objetos de impressão no dispositivo do usuário. A maioria dos aplicativos hoje pode enviar trabalhos de impressão para objetos de impressora. Essa configuração de política é necessária apenas para servidores que hospedam aplicativos legados que imprimem em portas LPT.

Observe que, embora o redirecionamento de porta COM do cliente seja bidirecional, o redirecionamento de porta LPT é apenas de saída e limitado a `\\client\LPT1` e `\\client\LPT2` dentro de uma sessão ICA.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta LPT
- Porcentagem de limite de largura de banda de redirecionamento de porta LPT

Configurações de política de impressão

A seção Impressão contém configurações de política para gerenciar a impressão do cliente.

Redirecionamento de impressora cliente

Essa configuração controla se as impressoras cliente são mapeadas para um servidor quando um usuário faz logon em uma sessão.

Por padrão, o mapeamento de impressora cliente é permitido. Se essa configuração estiver desabilitada, a impressora PDF para a sessão não será criada automaticamente.

Configurações de política relacionadas: criar impressoras cliente automaticamente

Impressora padrão

Essa configuração especifica como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como a impressora padrão para a sessão.

Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar a impressora padrão do usuário. Se você escolher essa opção, a impressora padrão não será salva no perfil e não será alterada de acordo com outras propriedades da sessão ou do cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é:

- A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e **Impressoras**.
- A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

Você pode usar essa opção para apresentar aos usuários a impressora mais próxima por meio das configurações de perfil (conhecido como impressão por proximidade).

Atribuições de impressora

Essa configuração oferece uma alternativa às configurações de Impressora padrão e Impressoras de sessão. Use as configurações individuais de Impressora padrão e Impressoras de sessão para configurar comportamentos para um site, grupo grande ou unidade organizacional. Use a

configuração **Atribuições de impressora** para atribuir um grande grupo de impressoras a vários usuários.

Essa configuração especifica como a impressora padrão nos dispositivos de usuário listados é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como a impressora padrão para a sessão.

Também especifica as impressoras de rede a serem criadas automaticamente em uma sessão para cada dispositivo de usuário. Por padrão, nenhuma impressora é especificada.

- Ao definir o valor da impressora padrão:

  Para usar a impressora padrão atual para o dispositivo de usuário, selecione Não ajustar.

  Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar. Se você escolher esta opção, a impressora padrão não será salva no perfil e não mudará de acordo com outras propriedades da sessão ou do cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é uma das seguintes:

  - A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e Impressoras.
  - A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

- Ao definir o valor das impressoras de sessão: para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Depois de 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

Essa configuração especifica os eventos que são registrados durante o processo de criação automática da 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.

- **Servidor de Impressão Windows:** Compartilha uma ou mais impressoras de rede. Ele também possui os drivers de impressora nativos necessários para usar as impressoras de rede.
- **Servidor de Impressão Universal:** Um Servidor de Impressão Windows onde o software Citrix Universal Print Server foi instalado.

Ao usar um 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 nele.

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 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. No Citrix Studio, navegar até a guia **Policies**.
2. Habilite a política de impressão de sessão na caixa de diálogo **Edit Policy**.
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 aparecer 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 faltando no servidor Citrix Virtual Apps ou a política foi criada, mas não habilitada.

> **Nota:**
>
> Se o driver da impressora não tiver sido instalado no servidor Citrix Virtual Apps, você poderá cometer o erro mais comum com impressoras de sessão, onde os administradores esquecem de instalar o driver da impressora no servidor Citrix Virtual Apps.

5. Inicie o desktop publicado e adicione manualmente a impressora de sessão em **Dispositivos e Impressoras > Painel de Controle**.
6. Se isso falhar, investigue a comunicação entre o servidor Citrix Virtual Apps e o servidor de impressão. Considere executar um teste com RDP.

Aguardar a criação das impressoras

Habilite este recurso de forma diferente, dependendo se é para Citrix Virtual Desktops™ ou Citrix Virtual Apps. Use a política no Delivery Controller para habilitar o recurso no Citrix Virtual Desktops. Use um cmdlet do PowerShell no Delivery Controller para habilitar o recurso no Citrix Virtual Apps.

Aguardar a criação de impressoras (Desktop de Servidor):

Esta configuração permite um atraso na conexão a uma sessão para que as impressoras redirecionadas pelo cliente possam ser criadas automaticamente.

Por padrão, não ocorre um atraso na conexão.

Aguardar a criação de impressoras (Citrix Virtual Apps):

A configuração do seguinte cmdlet do PowerShell permite um atraso na conexão a aplicativos virtuais criados em desktops de servidor para que as impressoras redirecionadas pelo cliente possam ser criadas automaticamente.

```
Set-BrokerApplication -Name <VirualAppName> -WaitForPrinterCreation $true
```

Por padrão, não ocorre um atraso na conexão.

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 de 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 a impressora padrão no dispositivo do usuário.
- **Criar automaticamente apenas impressoras cliente locais (não de rede)** cria automaticamente apenas impressoras conectadas diretamente ao dispositivo do usuário através de uma porta LPT, COM, USB, TCP/IP ou outra porta local.
- **Não criar automaticamente impressoras cliente** desativa a criação automática para todas as impressoras cliente quando os usuários fazem logon. A escolha desta opção faz com que as configurações dos Serviços de Área de Trabalho Remota (RDS) para criação automática de impressoras cliente substituam esta configuração em políticas de prioridade inferior.

CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL GENÉRICA

Esta configuração habilita ou desabilita a criação automática do objeto de Impressora Universal™ genérica da Citrix para sessões onde um dispositivo de usuário compatível com Impressão Universal está em uso.

Por padrão, o objeto de Impressora Universal genérica não é criado automaticamente.

As seguintes configurações de política estão relacionadas:

- Uso do driver de impressão universal
- Preferência de driver universal

CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL PDF

Esta configuração habilita ou desabilita a criação automática da impressora PDF do Citrix para sessões que usam o aplicativo Citrix Workspace para Windows (a partir do VDA 7.19), o aplicativo Citrix Workspace para HTML5 ou o aplicativo Citrix Workspace para Chrome.

Por padrão, a impressora PDF do 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 retroativa com nomes de impressoras herdados, conforme presentes nas versões XenApp e XenDesktop do produto. Você pode usar esta opção com as versões atuais do produto Citrix Virtual Apps and Desktops. Um exemplo de nome de impressora herdado é "Cliente/nomedocliente#/HPLaserJet 4." Esta opção é menos segura.

Ao usar a impressora PDF do Citrix em uma sessão iniciada a partir do aplicativo Citrix Workspace™ para HTML5, defina a configuração **Nomes de impressoras cliente** como padrão ou selecione **Nomes de impressoras padrão**. Se você selecionar **Nomes de impressoras herdados**, o aplicativo Citrix Workspace para HTML5 não oferece suporte à opção Impressora PDF do Citrix.

CONEXÕES DIRETAS A SERVIDORES DE IMPRESSÃO

Essa configuração habilita ou desabilita conexões diretas do desktop virtual ou servidor que hospeda aplicativos para um servidor de impressão para impressoras cliente hospedadas em um compartilhamento de rede acessível.

Por padrão, as conexões diretas são habilitadas.

Habilite as conexões diretas se o servidor de impressão de rede não estiver em uma WAN do desktop virtual ou servidor que hospeda aplicativos. A comunicação direta resulta em impressão mais rápida se o servidor de impressão de rede e o desktop virtual ou servidor que hospeda aplicativos 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 da 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 é definida para excluir o Microsoft OneNote e o XPS Document Writer da lista de impressoras cliente criadas automaticamente.

Ao definir regras de substituição de driver, você pode permitir ou impedir que impressoras sejam criadas com o driver especificado. Além disso, você pode permitir que impressoras criadas usem apenas drivers de impressão universais. A substituição de driver substitui ou mapeia nomes de driver de impressora fornecidos pelo dispositivo do usuário, substituindo um driver equivalente no servidor. Isso dá aos aplicativos do servidor acesso a impressoras cliente que têm os mesmos drivers que o servidor, mas nomes de driver diferentes.

Você pode adicionar um mapeamento de driver, editar um mapeamento existente, substituir configurações personalizadas para um mapeamento, remover um mapeamento ou alterar a ordem das entradas de driver na lista. Ao adicionar um mapeamento, insira o nome do driver da impressora cliente e selecione o driver do servidor que 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 têm um perfil obrigatório ou de roaming que não é salvo. Escolha esta opção somente se todos os servidores em seu farm estiverem executando o XenApp 5 ou superior e seus usuários estiverem usando plug-ins online Citrix versões 9 a 12.x, ou Citrix Receiver 3.x.

- Retido apenas no perfil do usuário é para dispositivos de usuário limitados por 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. Use esta opção com o MetaFrame Presentation Server 3.0 ou anterior e o MetaFrame Presentation Server Client 8.x ou anterior. Observe que isso é aplicável apenas se um perfil de roaming dos Serviços de Área de Trabalho Remota (RDS) for usado.
- Mantido no perfil somente 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 verificação do sistema.
- Não reter propriedades da impressora impede o armazenamento de propriedades da impressora.

IMPRESSORAS CLIENTE RETIDAS E RESTAURADAS

Esta configuração ativa ou desativa a retenção e a recriação de impressoras no dispositivo do usuário. Por padrão, as impressoras cliente são retidas e restauradas automaticamente.

Impressoras retidas são impressoras criadas pelo usuário que são criadas novamente, ou lembradas, no início da próxima sessão. Quando o Citrix Virtual Apps™ recria uma impressora retida, ele considera todas as configurações de política, exceto a configuração **Criar impressoras cliente automaticamente**.

Impressoras restauradas são impressoras totalmente personalizadas por um administrador, com um estado salvo que está permanentemente anexado a uma porta cliente.

DRIVER DE IMPRESSORA UNIVERSAL PDF CITRIX

O driver de Impressora Universal PDF Citrix permite que os usuários imprimam documentos abertos com aplicativos hospedados ou aplicativos em execução em desktops virtuais fornecidos pelo Citrix Virtual Apps and Desktops. Quando um usuário seleciona a opção **Impressora PDF Citrix**, 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 ativada, configurada e definida como padrão usando uma Política Citrix. A opção **Impressora PDF Citrix** 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** contém configurações de política relacionadas a drivers de impressora.

INSTALAÇÃO AUTOMÁTICA DE DRIVERS DE IMPRESSORA INTEGRADOS

> **Nota**
>
> Esta política não oferece suporte a VDAs nesta versão.

> Essa configuração habilita ou desabilita a instalação automática de drivers de impressora do conjunto de drivers internos do Windows ou de pacotes de drivers preparados no host usando pnputil.exe /a.

Por padrão, esses drivers são instalados conforme necessário.

PREFERÊNCIA DE DRIVER UNIVERSAL

Essa configuração especifica a ordem em que os drivers de impressora universais são usados, começando pela 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, potencialmente simplificando 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:

- 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 no logon. Se o driver solicitado não estiver disponível, a impressora cliente não poderá ser criada automaticamente.
- 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** contém configurações de política para gerenciar o Universal Print Server.

CONJUNTO DE CIFRAS SSL

Esta configuração especifica o conjunto de conjuntos de cifras SSL/TLS usados pelo 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

Esta configuração possui os seguintes valores: ALL, COM ou GOV.

Os conjuntos de cifras correspondentes a cada valor estão listados abaixo:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

MODO DE CONFORMIDADE SSL

Esta configuração especifica o nível de conformidade com a Publicação Especial 800-52 do NIST que é usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão criptografados (CGP).

Valor padrão: Nenhum.

Esta configuração possui os seguintes valores:

Nenhum.

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade padrão.

SP800-52.

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade da Publicação Especial 800-52 do NIST.

SSL ATIVADO

Esta configuração especifica se SSL/TLS é usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão (CGP) e para conexões de serviço web (HTTP/SOAP).

Quando você define **Ativar Servidor de Impressão Universal** como **Ativado com fallback para impressão remota nativa do Windows**, as conexões de fallback são feitas pelo Provedor de Impressão de Rede do Microsoft Windows. Esta configuração não afeta essas conexões de fallback.

Valor padrão: Desativado

Esta configuração possui os seguintes valores:

Ativado.

O Universal Print Client usa SSL/TLS para se conectar ao Universal Print Server.

Desativado.

O Universal Print Client usa SSL/TLS para se conectar ao Universal Print Server.

MODO FIPS SSL

Essa configuração especifica se o módulo criptográfico SSL/TLS usado pelo Universal Print Client para conexões de fluxo de dados de impressão (CGP) será executado no modo FIPS.

Valor padrão: Desativado

Esta configuração possui os seguintes valores:

Ativado.

O modo FIPS está ativado.

Desativado.

O modo FIPS está desativado.

VERSÃO DO PROTOCOLO SSL

Essa configuração especifica a versão do protocolo SSL/TLS usada pelo Universal Print Client.

Valor padrão: TODOS

Esta configuração tem os seguintes valores:

TODOS.

Use as versões TLS 1.0, 1.1 ou 1.2.

TLSv1.

Use a versão TLS 1.0.

TLSv1.1.

Use a versão TLS 1.1.

TLSv1.2.

Use a versão TLS 1.2.

PORTA SSL UNIVERSAL PRINT SERVER DE FLUXO DE DADOS DE IMPRESSÃO CRIPTOGRAFADO (CGP)

Esta configuração especifica o número da porta TCP da porta SSL Universal Print Server de fluxo de dados de impressão criptografado (CGP). Esta porta recebe dados para trabalhos de impressão.

Valor padrão: 443

PORTA SSL UNIVERSAL PRINT SERVER DE SERVIÇO WEB CRIPTOGRAFADO (HTTPS/SOAP)

Esta configuração especifica o número da porta TCP da porta SSL Universal Print Server de serviço web criptografado (HTTPS/SOAP). Esta porta recebe dados para comandos de impressão.

Valor padrão: 8443

HABILITAR UNIVERSAL PRINT SERVER

Esta configuração habilita ou desabilita o recurso Universal Print Server na área de trabalho virtual ou no servidor que hospeda aplicativos. Aplique esta configuração de política a Unidades Organizacionais (OUs) que contêm a área de trabalho virtual ou o servidor que hospeda aplicativos.

Por padrão, o Universal Print Server está desabilitado.

Ao adicionar esta configuração a uma política, selecione uma das seguintes opções:

- **Habilitado com fallback para impressão remota nativa do Windows**. As conexões de impressora de rede são atendidas pelo Universal Print Server, 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**. As conexões de impressora de rede são atendidas exclusivamente pelo Universal Print Server. Se o Universal Print Server estiver indisponível, a conexão da impressora de rede falhará. Esta configuração desabilita efetivamente a impressão em rede através do Provedor de Impressão do Windows. Impressoras criadas anteriormente com o Provedor de Impressão do Windows não são criadas enquanto uma política que contém esta configuração está 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 nativa do Windows.

PORTA DO FLUXO DE DADOS DE IMPRESSÃO DO UNIVERSAL PRINT SERVER (CGP)

Esta configuração especifica o número da porta TCP usado pelo ouvinte 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.

Números de porta válidos devem estar no intervalo de 1 a 65535.

LIMITE DE LARGURA DE BANDA DE ENTRADA DO FLUXO DE IMPRESSÃO DO UNIVERSAL PRINT SERVER (KBPS)

Esta configuração especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão entregues de cada trabalho de impressão para o Universal Print Server usando CGP. Aplique esta configuração de política a OUs que contêm a área de trabalho virtual ou o servidor que hospeda aplicativos.

Por padrão, o valor é 0, o que especifica nenhum limite superior.

PORTA DO SERVIÇO WEB DO UNIVERSAL PRINT SERVER (HTTP/SOAP)

Esta configuração especifica o número da porta TCP usado pelo ouvinte do serviço web (HTTP/SOAP) do Universal Print Server. O Universal Print Server é um componente opcional que permite o uso de drivers de impressão universais da Citrix para cenários de impressão em rede. Quando o Universal Print Server é usado, os comandos de impressão são enviados dos hosts do Citrix Virtual Apps and Desktops para o Universal Print Server via SOAP sobre HTTP. Esta configuração modifica a porta TCP padrão na qual o Universal Print Server escuta as solicitações HTTP/SOAP de entrada.

Você deve configurar a porta HTTP do host e do servidor de impressão de forma idêntica. Se você não configurar as portas de forma idêntica, o software do host não se conectará ao Universal Print

Server. Esta configuração altera o VDA no Citrix Virtual Apps and Desktops. Além disso, você deve alterar a porta padrão no Universal Print Server.

Por padrão, o número da porta é definido como 8080.

Os números de porta válidos devem estar no intervalo de 0 a 65535.

UNIVERSAL PRINT SERVERS PARA BALANCEAMENTO DE CARGA

Esta configuração lista os Universal Print Servers a serem usados para balancear a carga das conexões de impressora estabelecidas no início da sessão, após avaliar outras configurações de política de impressão da Citrix®. Para otimizar o tempo de criação da impressora, a Citrix recomenda que todos os servidores de impressão tenham o mesmo conjunto de impressoras compartilhadas. Não há limite superior para o número de servidores de impressão que podem ser adicionados para balanceamento de carga.

Esta configuração também implementa a detecção de failover do servidor de impressão e a recuperação de conexões de impressora. Os servidores de impressão são verificados periodicamente quanto à disponibilidade. Se uma falha de servidor for detectada, esse servidor será removido do esquema de balanceamento de carga, e as conexões de impressora nesse servidor serão 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 contém 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).

Configurações de política de impressão universal

A seção **Impressão Universal** contém 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 essa configuração a uma política, selecione uma opção:

- Reprocessar EMFs para impressora força o arquivo de spool EMF a ser reprocessado e enviado através do subsistema GDI no dispositivo do usuário. Você pode usar esta configuração para drivers que exigem reprocessamento de EMF, mas que podem não ser selecionados automaticamente em uma sessão.
- Enviar diretamente para a impressora, quando usado com o driver de impressão Citrix Universal™, garante que os registros EMF sejam enviados e entregues ao dispositivo do usuário para processamento. Normalmente, esses arquivos de spool EMF são injetados diretamente na fila de spool do cliente. Para impressoras e drivers compatíveis com o formato EMF, este é o método de impressão mais rápido.

LIMITE DE COMPACTAÇÃO DE IMAGEM DE IMPRESSÃO UNIVERSAL

Essa configuração especifica a qualidade máxima e o nível mínimo de compactação disponíveis 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 desativada apenas para impressão EMF.

Ao adicionar essa configuração a uma política, selecione uma opção:

- Nenhuma compactação
- Melhor qualidade (compactação sem perdas)
- Alta qualidade
- Qualidade padrão
- Qualidade reduzida (compressão máxima)

Ao adicionar esta configuração a uma política que inclui a configuração Padrões de otimização de impressão universal, esteja ciente do seguinte:

- Se o nível de compactação na configuração Limite de compactação de imagem de impressão universal for inferior ao nível definido na configuração Padrões de otimização de impressão universal, as imagens serão 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

Esta configuração especifica os valores padrão para otimização de impressão quando o driver de impressão universal é criado para uma sessão.

- A Qualidade de imagem desejada especifica o limite de 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 ou não ser armazenadas em cache, garantindo que cada imagem ou fonte exclusiva seja enviada à impressora apenas uma vez. Por padrão, imagens e fontes incorporadas são armazenadas em cache. Observe que essas configurações se aplicam somente se o dispositivo do usuário suportar esse comportamento.
- Permitir que não administradores modifiquem essas configurações especifica se os usuários podem ou não alterar as configurações padrão de otimização de impressão em uma sessão. 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:

- Se o nível de compactação na configuração Limite de compactação de imagem de impressão universal for inferior ao nível definido na configuração Padrões de otimização de impressão universal, as imagens serão compactadas no nível definido na configuração Limites de compactação de imagem de impressão universal.
- Se a compressão estiver desativada, as opções Qualidade de imagem desejada e Ativar compressão 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 ou não 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 máximo de pontos por polegada (dpi) disponível para gerar saída impressa em uma sessão.

Por padrão, Sem Limite está ativado, o que significa que os usuários podem selecionar a qualidade de impressão máxima permitida pela impressora à qual se conectam.

Se esta configuração for configurada, ela limita a qualidade de impressão máxima 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 são restritos a imprimir com uma qualidade máxima de 600 DPI e a configuração Qualidade de Impressão na guia Avançado da caixa de diálogo Impressora Universal mostra as configurações de resolução apenas até e incluindo Qualidade Média (600 DPI).

Ao adicionar esta configuração a uma política, selecione uma opção:

- Rascunho (150 DPI)
- Baixa Resolução (300 DPI)
- Média Resolução (600 DPI)
- Alta Resolução (1200 DPI)
- Sem Limite

Configurações de política de segurança

A seção Segurança contém a configuração de política para configurar a criptografia de sessão e a criptografia de dados de logon.

Nível mínimo de criptografia SecureICA

Essa configuração especifica o nível mínimo no qual criptografar os dados da sessão enviados entre o servidor e um dispositivo de usuário.

Importante: Para o Virtual Delivery Agent 7.x, essa 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 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 Grupo de Entrega do VDA. Se Habilitar Secure ICA for selecionado para o Grupo de Entrega, os dados da sessão serão criptografados usando criptografia RC5 (128 bits). Se Habilitar Secure ICA não for selecionado para o Grupo de Entrega, os dados da sessão serão criptografados com criptografia Básica.

Ao adicionar essa 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. Se um nível de criptografia de prioridade mais alta for definido em um servidor ou dispositivo de usuário, as configurações que você especificar para recursos publicados poderão 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 isso 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, que 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; e chaves de sessão separadas são usadas para o tráfego de e para o Virtual Delivery Agent. Portanto, existem 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 do servidor

A seção Limites do Servidor contém a configuração de política para controlar conexões ociosas.

Intervalo do temporizador de inatividade do servidor

Esta configuração determina, em milissegundos, por quanto tempo uma sessão de usuário ininterrupta é mantida se não houver entrada do usuário.

Por padrão, as conexões ociosas não são desconectadas (intervalo do temporizador de inatividade do servidor = 0). A Citrix® recomenda definir este valor para um mínimo de 60000 milissegundos (60 segundos).

Para exibir a política, selecione **Múltiplas Versões**, desmarque as versões do SO de sessão única e, em seguida, selecione **Limites do Servidor**.

> **Nota**

> Quando esta configuração de política é usada, uma caixa de diálogo "Tempo limite de inatividade expirado" pode aparecer para os usuários quando a sessão estiver ociosa pelo tempo especificado. As configurações de política da Citrix não controlam esta mensagem da caixa de diálogo da Microsoft. Para obter mais informações, consulte `<http://support.citrix.com/article/CTX118618>`.

Configurações de política de limites de sessão

A seção **Limites de Sessão** inclui configurações de política que controlam por quanto tempo as sessões permanecem conectadas antes de serem forçadas a fazer logoff.

> **Importante:**
>
> - As configurações descritas neste artigo não se aplicam a máquinas que executam VDAs de várias sessões. Para obter mais informações sobre como configurar limites de tempo de sessão para máquinas que executam VDAs de várias sessões, consulte Microsoft KB - Limites de Tempo de Sessão.
> - A partir do Windows Server 2012, o termo *Serviços de Terminal* mencionado em Microsoft KB - Limites de Tempo de Sessão refere-se a *Serviço de Área de Trabalho Remota*.

Temporizador de sessão desconectada

Esta configuração habilita ou desabilita:

- Um temporizador que especifica por quanto tempo uma área de trabalho desconectada e bloqueada permanece bloqueada antes que a sessão seja desconectada.

Se este temporizador estiver habilitado, a sessão desconectada será desconectada quando o temporizador expirar.

Por padrão, as sessões desconectadas não são desconectadas.

Temporizador de sessão desconectada do Remote PC Access

Esta configuração habilita ou desabilita um temporizador que desconecta uma sessão de usuário desconectada após o temporizador expirar. Se você habilitar esta configuração, use a configuração **Intervalo do temporizador de sessão desconectada** para especificar quantos

minutos uma área de trabalho desconectada pode permanecer bloqueada antes que a sessão do usuário seja desconectada.

Por padrão, esta configuração está desabilitada.

Intervalo do temporizador de sessão desconectada

Esta configuração especifica quantos minutos uma área de trabalho desconectada e bloqueada pode permanecer bloqueada antes que a sessão seja desconectada.

Por padrão, o período de tempo é de 1.440 minutos (24 horas).

Temporizador de conexão de sessão

Esta configuração habilita ou desabilita um temporizador que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop. Se este temporizador estiver habilitado, a sessão é desconectada ou encerrada quando o temporizador expira. A configuração da Microsoft **Encerrar sessão quando os limites de tempo forem atingidos** determina o próximo estado para a sessão.

Por padrão, esse temporizador está desabilitado.

Intervalo do temporizador de conexão de sessão

Esta configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e um desktop.

Por padrão, a duração máxima é de 1.440 minutos (24 horas).

Temporizador de 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 de dispositivo de usuário a um desktop é mantida.

Quando este temporizador expira, a sessão é colocada no estado desconectado e o **temporizador de sessão desconectada** é aplicado. Se o **temporizador de sessão desconectada** estiver desabilitado, a sessão não é encerrada.

Por padrão, esse temporizador está habilitado.

Intervalo do temporizador de inatividade da sessão

Quando não há entrada do usuário, essa 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).

> **Nota:**
>
> A partir da versão 2203 LTSR CU2, você pode configurar as seguintes configurações de limite de tempo de sessão para máquinas que executam VDAs de várias sessões.

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 encerrada. Por padrão, esse temporizador está desabilitado e as sessões desconectadas não são encerradas.

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 de tempo é de 1440 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 – Multi-sessão

Essa configuração habilita ou desabilita um temporizador para determinar a duração máxima de uma conexão ociosa entre um dispositivo de usuário e um servidor de terminal. Por padrão, esse temporizador está desabilitado.

Intervalo do temporizador de inatividade da sessão – Multi-sessão

Essa 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).

Observação:

Espera-se que as configurações de temporizador para máquinas de várias sessões configuradas usando políticas Citrix® substituam as configurações de temporizador configuradas por meio 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

Esta 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 Citrix 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 Citrix Studio substitui o Objeto de Política de Grupo do Citrix Receiver™ nos clientes. As atualizações dessas políticas no 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 Studio.
- Citrix Receivers para Windows anteriores a 4.7 - Defina as políticas no 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 estiver em uso, você deve selecionar **Habilitar confiabilidade da sessão** no Citrix StoreFront > **Gerenciar Citrix Gateways** / **Secure Ticket Authority** para fazer proxy de conexões ICA.

> Para desabilitar a confiabilidade da sessão:

1. Inicie o Citrix Studio.
2. Abra a política **Conexões de confiabilidade da sessão**.
3. Defina a política como **Proibido**.



Número da porta de confiabilidade da sessão

Essa 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.

Para alterar o número da porta de confiabilidade da sessão:

1. Inicie o Citrix Studio.
2. Abra a política **Número da porta de confiabilidade da sessão**.
3. Edite o número da porta.
4. Clique em **OK**.

Tempo limite de confiabilidade da sessão

Essa configuração especifica a duração, em segundos. Esse tempo é o tempo que o proxy de confiabilidade da sessão aguarda a reconexão de um usuário 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.

Para alterar o tempo limite de confiabilidade da sessão:

1. Inicie o Citrix Studio.
2. Abra a política de **tempo limite de confiabilidade da sessão**.
3. Edite o valor do tempo limite.
4. Clique em **OK**.

Configurações de política de marca d'água de sessão

A seção de marca d'água de sessão contém configurações de política para configurar esse recurso. Habilitar esse 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 de sessão

Quando você habilita essa 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 de esta estar habilitada.

Por padrão, a marca d'água de sessão está desabilitada.

Incluir endereço IP do cliente

Quando você habilita essa 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 essa configuração, a marca d'água da sessão exibe uma hora 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 hora da conexão está desabilitado.

Incluir nome de usuário de logon

Quando você habilita essa configuração, a sessão exibe o nome de usuário de logon atual como uma marca d'água. O formato de exibição é NOME_DE_USUÁRIO@NOME_DE_DOMÍNIO. Recomendamos que o nome de usuário tenha no máximo 20 caracteres. Quando um nome de usuário tem mais de 20 caracteres, podem ocorrer fontes de caracteres excessivamente pequenas ou truncamento, diminuindo 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 especifica uma string de texto personalizada (por exemplo, o nome da empresa) para exibir na marca d'água da sessão. Quando você configura uma string não vazia, ela exibe o texto em uma nova linha, anexando outras informações habilitadas na marca d'água. O texto personalizado da marca d'água tem um máximo de 25 caracteres Unicode. Se você configurar uma string mais longa, ela será truncada para 25 caracteres.

Não há texto padrão.

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 contém configurações de política relacionadas ao uso do horário local nas sessões.

Estimar hora local para clientes legados

Essa configuração habilita ou desabilita a estimativa do fuso horário local de dispositivos de 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. Quando usada com Citrix Receivers que enviam informações detalhadas de fuso horário para o servidor, como versões compatíveis do Citrix Receiver™ para Windows, essa configuração não tem efeito.

Restaurar fuso horário do SO da área de trabalho na desconexão ou logoff da sessão

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 quando o usuário se desconecta ou faz logoff. Se você habilitar essa configuração, o VDA restaura o fuso horário da máquina para sua configuração original quando o usuário se desconecta ou faz logoff. Para que essa configuração tenha efeito, defina **Usar horário 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 Dispositivo e Recurso**.

Se você estiver usando um 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, **Usuários** estão incluídos na Atribuição de Direitos de Usuário **Alterar o fuso horário**, embora não em um SO de múltiplas sessões. Em um SO de múltiplas sessões, o fuso horário sincroniza usando a seguinte política de grupo: Configuração do Computador\Modelos Administrativos\Componentes do Windows\Serviços de Área de Trabalho Remota\Host da Sessão da Área de Trabalho Remota\Redirecionamento de Dispositivo e Recurso\Permitir redirecionamento de fuso horário. Esta política não se aplica quando o Servidor não é um Host da Sessão da Área de Trabalho Remota no VDA de SO de múltiplas sessões (instalado com o comando `/`

> `ServerVDI`). Em um SO de múltiplas sessões, por padrão e por design, os usuários não têm o direito local de alterar o fuso horário.

Configurações de política de dispositivos USB

A seção **Dispositivos USB** contém configurações de política para gerenciar o redirecionamento de arquivos para dispositivos USB.

Regras de otimização de dispositivos USB do cliente

As regras de otimização de dispositivos USB do cliente podem ser aplicadas aos dispositivos para desativar a otimização ou para alterar o modo de otimização.

Quando um usuário conecta um dispositivo de entrada USB, o host verifica se as configurações da **política USB** permitem o dispositivo. Se o dispositivo for permitido, o host verifica as **regras de otimização de dispositivos USB do cliente** para o dispositivo. Se nenhuma regra for especificada, o dispositivo não será otimizado. O modo de captura (04) é o modo recomendado para dispositivos de assinatura. Para outros dispositivos que apresentam desempenho degradado com maior latência, 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 de assinatura 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 da série de produtos de mesas digitalizadoras e tablets de assinatura Wacom STU foi pré-configurado na instalação das políticas do Citrix Virtual Apps and Desktops™.
- Dispositivos de assinatura funcionam em todo o Citrix Virtual Apps and Desktops e não exigem um driver para serem usados como um dispositivo de assinatura. A Wacom possui mais software que pode ser instalado para personalizar ainda mais o dispositivo. Consulte `<http://www.wacom.com/>`.
- 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 a classe=**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.
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 em modo de captura

Mode=00000002 VID=067B PID=1230 class=03 #Dispositivo de entrada operando em 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 desativada (padrão)

Mode=00000200 VID=067B PID=1230 # Otimização de configuração do dispositivo ativada

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 do pad de assinatura.
3. Vá para **Painel de Controle > Wacom STU Display > STU430** ou **STU530** e selecione a guia para o 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 pad de assinatura, 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 regras de redirecionamento para dispositivos USB.

Por padrão, nenhuma regra é especificada.

Quando um usuário conecta um dispositivo USB, o dispositivo host o verifica em relação a cada regra de política, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva. Se a primeira correspondência for uma regra de Permissão, o dispositivo é remotado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo estará disponível apenas para o desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

As regras de política têm o formato {Allow:`|`Deny:} seguido por um conjunto de expressões tag=valor separadas por espaço 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 puras 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 # Mass Storage
- Para criar uma regra que nega todos os dispositivos USB, use "DENY:" sem outras tags.

Redirecionamento de dispositivo plug and play USB do cliente

Essa configuração permite ou impede que dispositivos plug-and-play, como câmeras ou dispositivos de ponto de venda (POS), sejam usados em uma sessão de cliente.

Por padrão, o redirecionamento de dispositivo 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 e as configurações de preferência do usuário USB estão definidas para conectar dispositivos USB automaticamente.

Nota:

No Receiver para Windows 4.2, os dispositivos USB também são redirecionados automaticamente ao operar no modo Desktop Appliance, e a barra de conexão não está presente. Em versões anteriores do Citrix Receiver para Windows, os dispositivos USB também são redirecionados automaticamente ao operar em um modo de dispositivo de desktop ou com 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 Registry Editor 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 Registry Editor possam ser resolvidos. Use o Registry Editor por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

CONFIGURAÇÕES DE PREFERÊNCIAS DO USUÁRIO PARA REDIRECIONAMENTO AUTOMÁTICO DE DISPOSITIVOS USB

Política:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
2. Abra **Novos Dispositivos USB**, selecione **Habilitado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Habilitado** e clique em **OK**.

Citrix Receiver:

1. Vá para **Preferências do Citrix Receiver > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    - Quando uma sessão é iniciada, conectar dispositivos automaticamente
    - Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

Todas as chaves de registro e as alterações de política são aplicadas ao dispositivo cliente Windows.

REDIRECIONAMENTO DE IMPRESSORAS USB SIMPLES

A melhor solução para impressoras USB comuns é usar o Driver de Impressora Universal dedicado e o canal virtual para realizar a impressão. Por padrão, as impressoras USB comuns não são redirecionadas automaticamente.

As impressoras comuns são detectadas usando heurísticas, e espera-se que impressoras avançadas com funções de digitalização, por exemplo, precisem ser redirecionadas usando o suporte USB para funcionar completamente.

Use este registro para configurar se as impressoras comuns são redirecionadas automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Tipo: DWORD

Data: 00000000

O valor padrão é 0 (não redireciona automaticamente). Alterar o valor para qualquer número maior que zero habilita o suporte USB para redirecionar impressoras USB comuns.

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 COMUNS

Assim como as impressoras comuns, a melhor experiência do usuário é alcançada usando o canal virtual de áudio dedicado do ICA® para enviar dados de áudio de dispositivos de áudio comuns. No entanto, pode ser necessário redirecionar alguns dispositivos especiais usando o suporte USB. Heurísticas são usadas para determinar quais dispositivos são dispositivos de áudio comuns.

Use este registro no endpoint do cliente para configurar se os dispositivos de áudio comuns são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos de áudio USB simples com suporte USB.

Você pode usar políticas do Active Directory para implantar este valor na chave do Registro e substituir o valor não-política, se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: 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 de simplesmente ler ou gravar arquivos, para executar certas tarefas especiais, como gravar um CD/DVD ou acessar dispositivos de sistemas de arquivos criptografados, o dispositivo ainda pode precisar ser redirecionado usando o suporte USB genérico.

Heurísticas são usadas para determinar quais dispositivos são dispositivos de armazenamento simples. Use esta chave do 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 do Registro e substituir o valor não-política, se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

> **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

Pen drives 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 pen drive USB, obtenha a melhor experiência do usuário usando o canal virtual HDX dedicado de mapeamento de unidade cliente/ mapeamento dinâmico de pen drive que também realiza otimização.

O redirecionamento USB genérico é necessário para clientes não Windows (por exemplo, clientes Linux) e 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, pen drives USB com criptografia de hardware não podiam ser redirecionados de forma útil para sessões VDA de SO de sessão única ou SO de múltiplas sessões. Um novo aprimoramento de recurso introduzido no Citrix Virtual Apps and Desktops 7 1808 oferece suporte ao redirecionamento USB genérico de pen drives USB com criptografia de hardware para sessões VDA de SO de sessão única e SO de múltiplas sessões. Depois que o dispositivo é redirecionado, nenhuma de suas unidades aparece no cliente local. Portanto, se for necessário desbloquear a unidade, faça-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 executa a otimização. Esses dispositivos devem aderir aos padrões da indústria. Se um dispositivo não estiver em conformidade ou se não for usado de acordo com as intenções originais, 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 os 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 este 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 (como impressoras, áudio, vídeo, armazenamento e dispositivos de imagem estática) nem sempre correspondem ao que você deseja. Você pode querer controlar o redirecionamento automático de dispositivos que não estão listados acima. Você pode controlar o redirecionamento automático com base em cada dispositivo.

Por exemplo, o leitor de código de barras DemoTech 2.000 não precisa ser redirecionado usando o suporte USB. Ele tem um identificador de fornecedor de 12AB e um identificador de produto de 5678. Esses números hexadecimais podem ser encontrados no Gerenciador de Dispositivos.

Para evitar que isso seja redirecionado automaticamente, crie esta chave de registro específica do dispositivo:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dados: 00000000

Um valor de 0 impede que o dispositivo seja redirecionado automaticamente. Um valor diferente de zero indica que o dispositivo deve ser considerado para redirecionamento automático (sujeito às preferências do usuário). Há um único caractere de espaço entre os identificadores de fornecedor e produto.

Você também pode implantar este valor usando políticas do Active Directory para esta chave de registro. Ele substitui o valor não-política 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 mais gerais de AutoRedirectXXX explicados acima. As heurísticas padrão para dispositivos otimizados para Citrix podem interpretar um dispositivo como genérico. Portanto, defina o valor de AutoRedirect específico do dispositivo como 1 para redirecioná-lo automaticamente.

Configurações da política de lista de permissões de canais virtuais

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, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Mais caminhos executáveis podem ser listados, e os caminhos são separados por vírgulas.

Por exemplo,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

A partir do Citrix Virtual Apps and Desktops™ 7 2109, as listas de permissões de canais virtuais são ativadas por padrão.

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.

Configurações de política de exibição visual

A seção Exibição Visual contém configurações de política para controlar a qualidade das imagens enviadas de desktops virtuais para o dispositivo do usuário.

Profundidade de cor preferencial para gráficos simples

Essa configuração de política está disponível nas versões VDA 7.6 FP3 e posteriores. A opção de 8 bits está disponível nas versões VDA 7.12 e posteriores.

Essa configuração permite 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, ao custo de uma ligeira degradação na qualidade da imagem. A profundidade de cor de 8 bits não é suportada quando a configuração de política Usar codec de vídeo para compactação está definida como Para a tela inteira.

A profundidade de cor preferencial padrão é de 24 bits por pixel.

Os VDAs voltam para a profundidade de cor de 24 bits (padrão) se a configuração de 8 bits for aplicada na versão VDA 7.11 e anteriores.

Taxa de quadros alvo

Essa 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

Essa 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 pela 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 preservar dados de 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 do modo gráfico herdado está ativada.

Esta configuração especifica a qualidade mínima aceitável da imagem para o Adaptive Display. Quanto menos compactação for usada, maior será a qualidade das imagens exibidas. Escolha entre compactação Ultra Alta, Muito Alta, Alta, Normal ou Baixa.

Por padrão, isso é definido como Normal.

COMPACTAÇÃO DE IMAGEM EM MOVIMENTO

Esta configuração especifica se o Adaptive Display está ativado ou não. O Adaptive Display ajusta automaticamente a qualidade da imagem de vídeos e slides de transição em apresentações 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 modo gráfico herdado está ativado. Para as versões 7.6 FP1 e posteriores do VDA, esta configuração se aplica quando o modo gráfico herdado está ativado, ou quando o modo gráfico herdado está desativado e um codec de vídeo não é usado para compactar gráficos.

Quando o modo gráfico herdado está ativado, a sessão deve ser reiniciada para que as alterações de política entrem em vigor. O Adaptive Display é mutuamente exclusivo com o Progressive Display; ativar o Adaptive Display desativa o Progressive Display e vice-versa. No entanto, tanto o

Progressive Display quanto o Adaptive Display podem ser desativados ao mesmo tempo. O Progressive Display, como um recurso herdado, não é recomendado para XenApp ou XenDesktop. Definir o Nível de Limite Progressivo desativará o Adaptive Display.

NÍVEL DE COMPACTAÇÃO PROGRESSIVA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política do modo gráfico herdado está ativada.

Esta configuração 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 se torna disponível. Use compactação Muito Alta ou Ultra Alta para uma melhor visualização 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 desta 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 VDA 7.0 a 7.6, esta configuração se aplica somente quando o modo gráfico herdado está ativado. Para as versões VDA 7.6 FP1 e posteriores, esta configuração se aplica quando o modo gráfico herdado está desativado ou ativado.

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 ativa ou desativa 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 desativada.

Quando ativada, a compactação de cor extra é aplicada somente quando a largura de banda da conexão do cliente está abaixo do valor limite de compactação de cor extra. Quando a largura de banda da conexão do cliente está acima do valor limite ou a opção Desativado é selecionada, a compactação de cor extra 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 de modo gráfico herdado está ativada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão abaixo da qual a compactação de cor extra é aplicada. Se a largura de banda da conexão do cliente cair abaixo do valor definido, a compactação de cor extra, se ativada, 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 de modo gráfico herdado está ativada.

Esta configuração ativa ou desativa a redução da largura de banda além da compactação progressiva sem perda de qualidade da imagem, usando um algoritmo gráfico mais avançado, mas que exige mais CPU.

Por padrão, a compactação pesada está desativada.

Se ativada, 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 do modo gráfico herdado está ativada.

Esta configuração controla o grau de compressão com perdas usado em imagens entregues por conexões de cliente com largura de banda limitada. 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, talvez você não queira 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 do 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 de 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 de dispositivos WIA contém configurações de política para gerenciar o redirecionamento de scanner usando o Windows Image Acquisition (WIA).

Redirecionamento WIA

Dispositivos WIA, como câmeras digitais e scanners, se comunicam com aplicativos de processamento de imagem hospedados em servidor usando a estrutura WIA. 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 através do registro

> **Observação:**

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

> Para abrir o Editor do Registro, execute `regedit.exe` no servidor. Em seguida, navegar até a chave do registro para adicionar ou editar as configurações.

Dispositivos

Teclados Bloomberg

O Citrix Virtual Apps and Desktops™ oferece suporte aos teclados Bloomberg modelo 4 e modelo 3 starboard. Por padrão, o suporte para o teclado Bloomberg aprimorado está desabilitado.

Para habilitar o suporte ao teclado Bloomberg, defina o seguinte valor de registro na máquina cliente antes de iniciar uma conexão:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- Nome do valor: EnableBloombergHID
- Tipo de valor: DWORD

- Dados do valor: 0 = Desabilitar, 1 = Habilitar

Para obter mais informações, consulte Teclado Bloomberg.

Unidades de cliente mapeadas

Como precaução de segurança, quando um usuário faz logon no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades de cliente sem permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis localizados em unidades de cliente mapeadas, substitua esse padrão editando o registro no servidor.

Para permitir o acesso, edite o seguinte valor 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 permissão, 0 = Negar permissão em unidades mapeadas

A alteração entra em vigor para as sessões conectadas após a edição do registro.

Para obter mais informações, consulte Unidades de cliente mapeadas.

Canetas Microsoft Surface Pro e Surface Book

O Citrix Virtual Apps and Desktops oferece suporte à funcionalidade padrão de caneta com aplicativos baseados em Windows Ink. Por padrão, esse recurso está habilitado.

Para desabilitar ou habilitar esse recurso, defina o seguinte valor 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 permissão de aplicativos do Windows Image Acquisition

Essa configuração permite controlar quais aplicativos no VDA podem acessar o redirecionamento do scanner de Aquisição de Imagens do Windows.

Por padrão, nenhum aplicativo tem acesso à Aquisição de Imagens do Windows.

Para ajustar a Aquisição de Imagens do Windows para aplicativos no VDA, crie a seguinte configuração de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- Nome do valor: WIAAllowedProcesses

  Selecione e clique com o botão direito 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 Imagens do Windows. Forneça cada aplicativo em uma nova linha.

Quaisquer alterações a esta configuração entram em vigor na próxima vez que você iniciar uma sessão no VDA.

Geral

Configurar logon automático no VDA

Esta configuração permite habilitar ou desabilitar a configuração de política da Microsoft **Sempre solicitar senha** nos VDAs de SO de sessão única e SO de múltiplas sessões do Windows 10.

Se **Sempre solicitar senha** estiver habilitado, os usuários devem inserir credenciais no VDA ao iniciar uma sessão remota. Se esta configuração estiver desabilitada, os usuários se conectam automaticamente à sessão remota sem fornecer credenciais no VDA.

Por padrão, a configuração de política da Microsoft está desabilitada. Para habilitar ou desabilitar a configuração **Sempre solicitar senha**, defina o seguinte valor de registro no VDA:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- Nome do valor: AutoLogon
- Tipo de valor: DWORD
- Dados do valor:
  - 1 - 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.

Desativar aviso de tempo limite

Por padrão, usuários com sessões inativas ou ociosas recebem uma mensagem de aviso dois minutos antes que sua sessão seja desconectada automaticamente.

Esta configuração desabilita e remove a mensagem de aviso para usuários que atingem o limite de tempo limite de sessão ociosa em um SO de múltiplas sessões do Windows 2004 ou 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 está habilitada por padrão. Para desabilitar 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 para toda a máquina e afeta todas as sessões que se conectam de um cliente compatível.

Redirecionamento geral de conteúdo

Adicionar tipos de URL para redirecionamento do host para o cliente

Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL: HTTP, HTTPS, RTSP, RTSPU, PNM e MMS. Você pode adicionar tipos de URL à lista criando a seguinte chave de registro e valores 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. Se você habilitar o redirecionamento de pasta do cliente no servidor e o usuário o configurar no dispositivo do usuário, a parte do volume local especificada pelo usuário será redirecionada.

Para habilitar o redirecionamento de pasta do cliente no servidor, defina o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- Nome do valor: CFROnlyModeAvailable
- Tipo de valor: DWORD
- Dados do valor: 1

Para obter mais informações, consulte Redirecionamento de pasta do cliente.

Redirecionamento do host para o cliente para um conjunto específico de sites

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, defina o seguinte valor de registro no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: ValidSites
- Tipo de valor: REG_MULTI_SZ

- Dados do valor: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este 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: Estado da Sessão
- 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 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 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 uma URL da web não for redirecionada, o iniciador Citrix passará a URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente.

- Internet Explorer (Padrão)
  - Chave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome do valor: Padrão
  - 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: Padrão
  - 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: Padrão
  - Tipo de valor: REG_SZ

    - Dados do valor: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`
    - Chave: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - Nome do valor: Default
    - Tipo de valor: REG_SZ
    - Dados do valor: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`

- Microsoft Edge
    - Chave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
    - Nome do valor: Default
    - Tipo de valor: REG_SZ
    - Dados do valor: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`
    - Chave: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - Nome do valor: Default
    - Tipo de valor: REG_SZ
    - Dados do valor: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`

O Acesso a Aplicativos Locais para aplicativos publicados

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Para fornecer acesso a aplicativos publicados, defina o seguinte valor de registro no servidor:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- Nome do valor: ClientHostedAppsEnabled
- Tipo de valor: DWORD
- Dados do valor: 1 = Habilitar, 0 = Desabilitar

Para obter mais informações, consulte Acesso a Aplicativos Locais e redirecionamento de URL.

Gráficos

Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos POC de aceleração CUDA, habilite a seguinte configuração de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\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 multi-sessão 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 (Desativa o modo progressivo. Este valor é o padrão.)
  - 1 = Automático (Alterna com base nas condições da rede.)
  - 2 = Sempre ativado

Para obter mais informações, consulte Modo progressivo.

Renderização do Windows Presentation Foundation (WPF)

O HDX 3D Pro permite que aplicativos com uso intenso de gráficos executados em sessões do Windows Multi-session OS sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor.

Para habilitar a renderização de aplicativos WPF usando a GPU do servidor, crie a seguinte configuração no registro do servidor que executa o Windows multi-session OS:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook
- Nome do valor: EnableWPFHook
- Tipo de valor: DWORD
- Dados do valor: 00000001

Para obter mais informações, consulte Aceleração de GPU para Windows multi-session OS.

Multimídia

Evitar eco durante conferências multimídia

Citrix Virtual Apps and Desktops fornecem 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: DWORD
- 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 áudio. Como solução alternativa, adicione a seguinte chave de registro na máquina RDS e reinicie a máquina:

- Chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- Nome do valor: EnableSvchostMitigationPolicy
- Tipo de valor: DWORD
- Dados do valor: 0

Para obter mais informações, consulte Recursos de áudio.

Redirecionamento de conteúdo do navegador e DPI

Ao usar o redirecionamento de conteúdo do navegador com o DPI (dimensionamento) definido para qualquer valor acima de 100% na máquina do usuário, a tela de conteúdo do navegador redirecionado é exibida incorretamente. Para evitar o problema, desative a aceleração de GPU do redirecionamento de conteúdo do navegador para o Chrome criando o seguinte valor de registro na máquina do usuário:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- Nome do valor: GPU
- Tipo de valor: DWORD
- Dados do valor: 0

Para obter mais informações, consulte Redirecionamento de conteúdo do navegador e DPI.

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. O Citrix Virtual Apps and Desktops suporta resoluções de webcam de até 1920x1080. Para desativar e ativar o streaming de webcam de alta definição, adicione o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXRealTime
- Nome do valor: Enable_HighDefWebcam
- Tipo de valor: DWORD
- Dados do valor:
  - 0 = Desabilitar o streaming de webcam de alta definição

- 1 = Habilitar o streaming de webcam de alta definição

Resolução da webcam de alta definição

Se a negociação do tipo de mídia falhar, o HDX reverterá para a resolução padrão de 352x288 CIF. 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)

Largura de banda da webcam de alta definição

A compressão de vídeo da webcam HDX usa 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 o seguinte valor de registro no cliente:

- Chave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Nome do valor: TargetBitrate
- Tipo de valor: DWORD
- Dados do valor: 350000

Insira um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usarão 350000 bps por padrão.

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

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 às 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 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 = Habilitar somente áudio

Se o valor não estiver presente ou for definido como 0, o modo de fallback será habilitado. Este recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior. Para obter mais informações, consulte Otimização para Microsoft Teams.

Otimização para Microsoft Teams com Citrix App Layering™

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, implante esta chave de registro no Windows antes de instalar o Microsoft Teams com **ALLUSER**=1.

Crie uma chave de registro vazia chamada **PortICA** e mantenha o nome, tipo e dados do valor padrão.

- Chave para a versão de 32 bits do Editor do Registro: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- Chave para a versão de 64 bits do Editor do Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

Para obter mais informações, consulte Otimização para Microsoft Teams.

Logon único com Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

Essa configuração fornece logon único a um servidor web configurado com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA. Para habilitar o logon único, defina o seguinte valor de registro como 1:

- Chave:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  ou

  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- Nome do valor: WebBrowserRedirectionIwaSupport
- Tipo de valor: DWORD
- Dados do valor: 1

Para obter mais informações, consulte Logon único com Autenticação Integrada do Windows.

Cabeçalho de solicitação de user-agent

O cabeçalho user-agent ajuda a identificar as solicitações HTTP enviadas do redirecionamento de conteúdo do navegador. Essa configuração pode ser útil ao configurar regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas do redirecionamento de conteúdo do navegador, você poderá criar uma regra que contenha o cabeçalho user-agent para ignorar certos requisitos. Somente dispositivos Windows suportam o cabeçalho de solicitação de user-agent.

Por padrão, a string do cabeçalho de solicitação de user-agent está desabilitada. Para habilitar o cabeçalho user-agent para conteúdo renderizado pelo cliente, use o Editor do Registro.

Em cada cliente do aplicativo Citrix Workspace™ para Windows, defina uma das seguintes configurações de registro:

- Chave:
  - 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- Nome do valor: EnableCefUserAgentString
- Tipo de valor: DWORD
- Dados do valor: 1

Depois de adicionar o valor do registro, o cabeçalho user-agent contém o texto CitrixBCR/2102.1, onde 2102.1 é a versão do aplicativo Citrix Workspace para Windows.

Compressão de software da webcam

Se uma webcam suportar codificação de hardware, a compressão de vídeo HDX usa a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compressão de software, adicione o seguinte valor no 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 compactação de vídeo da webcam HDX.

Compressão de vídeo da webcam

A compactação 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 compactação da webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Este recurso é habilitado por padrão.

Para desabilitar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina o seguinte valor de registro no VDA.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- Nome do valor: OfferH264ToApp
- Tipo de valor: DWORD
- Dados do valor: 0

Para obter mais informações, consulte compactação de vídeo da webcam HDX.

Taxa de quadros de compactação 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 contém 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 de 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 as máquinas são gerenciadas pelo Workspace Environment Management, 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, isso 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 de 75% completa. 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 da 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 e define, em MB, o uso da memória abaixo do qual um servidor é considerado com carga zero.

Por padrão, isso é definido como 768 MB.

Configurações de política de gerenciamento de perfil

Configurações de política avançadas

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 no 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 nem aqui nem no arquivo .ini, nenhum processamento de Index.dat ocorrerá.

Desabilitar configuração automática

O Profile Management examina qualquer ambiente Citrix Virtual Desktops™, por exemplo, para a presença de vDisks pessoais, e configura a Política de Grupo de acordo. Apenas as políticas do Profile Management no estado Não Configurado são ajustadas, de modo que quaisquer personalizações que você tenha feito são preservadas.

Esta política permite acelerar a implantação e simplifica a otimização. Você não precisa configurar esta política. No entanto, você pode desabilitar a configuração automática ao fazer uma das seguintes ações:

- Atualizar para reter configurações de versões anteriores
- Solução de problemas

Você pode considerar a configuração automática como um verificador de configuração 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 Personal vDisk estiver em uso; caso contrário, habilitado.
Sempre armazenar em cache	Desabilitado	*Desabilitado* se o Personal vDisk estiver em uso; caso contrário, habilitado.
Excluir perfis armazenados em cache localmente no logoff	Ativado	*Desabilitado* se uma das seguintes situações ocorrer: Personal vDisk está em uso, Citrix Virtual Desktops está atribuído ou Citrix Virtual Desktops não está 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 padronizam 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 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 esta configuração não for configurada aqui, o valor do arquivo .ini é usado.

Se esta configuração não for configurada aqui nem no arquivo .ini, a configuração automática é 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 é exibida e os usuários são 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 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 depois 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 boa do banco de dados do índice de pesquisa. Quando uma tentativa de montar o banco de dados do índice de pesquisa falha devido à corrupção do banco de dados, o Profile Management reverte o banco de dados do índice de pesquisa para a última cópia boa conhecida.

> Nota:
>
> O Profile Management exclui o backup salvo anteriormente depois que um novo backup é salvo com sucesso. O backup consome o armazenamento VHDX disponível.

Habilitar gravação de várias sessões para contêineres de perfil

Habilita a gravação para contêineres de perfil em cenários de várias sessões. Se ativado, 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 contêiner de perfil FSLogix 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 **Try for read-write profile and fallback to read-only** no FSLogix.

Replicar armazenamentos de usuário

Permite replicar um armazenamento de usuário para vários caminhos a cada logon e logoff, além do caminho especificado pela política **Path to user store**. Para sincronizar os arquivos e pastas dos armazenamentos de usuário modificados durante uma sessão, habilite a gravação ativa (active write-back). Este recurso atualmente não oferece suporte a soluções de contêiner completas. Habilitar a política pode aumentar o I/O do sistema e pode prolongar os logoffs.

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 Windows Credential Manager. Recomendamos que você use o Workspace Environment Management para eliminar a necessidade de configurar as mesmas credenciais para cada máquina onde o Profile Management é executado. Se você usar o Windows Credential Manager, use a conta do Sistema Local para salvar as credenciais com segurança.

> **Observação:**

> Para garantir que as permissões NTFS sejam mantidas, você deve colocar o perfil inteiro em um contêiner de perfil.

> Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não for configurada nem aqui nem no arquivo .ini, ela será desabilitada por padrão.

Personalizar caminho de armazenamento para arquivos VHDX

O Profile Management oferece as seguintes políticas baseadas em VHDX: Contêiner de perfil, Roaming de índice de pesquisa para Outlook e 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.

Reanexar discos VHDX automaticamente nas sessões

Com esta política habilitada, o Profile Management garante um alto nível de estabilidade das políticas baseadas em VHDX. Por padrão, esta política está habilitada.

Quando esta política está habilitada, o Profile Management monitora os discos VHDX que estão em uso pelas políticas baseadas em VHDX. Se algum dos discos for desanexado, o Profile Management o reanexa automaticamente.

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 for definida 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 for definida aqui, o valor do arquivo .ini será usado. Se esta configuração não for definida 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. Se esta política estiver desabilitada ou não configurada em sistemas operacionais multi-sessão (como ambientes Citrix Virtual Apps), 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, ignorem qualquer processamento, façam logon e solucionem problemas no desktop que esteja apresentando problemas com o Profile Management.

Nota: Os logons de usuários de domínio podem estar sujeitos a restrições impostas pela associação a grupos, tipicamente para garantir a conformidade com o licenciamento do produto. Se esta política estiver desabilitada, o Profile Management não processará os logons de administradores locais. Se esta política não for configurada aqui, o valor do arquivo .ini será usado. Se esta política não for configurada aqui ou no arquivo .ini, os administradores não serão processados.

Caminho para o armazenamento de 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. Deve ser relativo ao diretório inicial (que é tipicamente configurado como o atributo #homeDirectory# para um usuário no Active Directory).
- Um caminho UNC. Geralmente especifica um compartilhamento de servidor ou um namespace DFS.

- Desabilitado ou não configurado. Neste caso, um valor de #homeDirectory#\Windows é assumido.

Os seguintes tipos de variáveis podem ser usados para esta política:

- Variáveis de ambiente do sistema entre sinais de porcentagem (por exemplo, %ProfVer%). As variáveis de ambiente do sistema geralmente exigem configuração extra.
- 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 sobre 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, de forma completa. 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$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!` pode expandir para `\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`

Importante: Quaisquer que sejam os atributos ou variáveis que você use, verifique se esta política se expande para a pasta um nível acima da pasta que contém NTUSER.DAT. Por exemplo, se este arquivo estiver contido em `\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`, defina o caminho para o armazenamento do usuário como `\\server\profiles$\JohnSmith.Finance\Win8x64` (não a subpasta \UPM_Profile).

Para obter mais informações sobre o uso de variáveis ao especificar o caminho para o armazenamento do 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 do usuário estiver desabilitado, as configurações do usuário serão salvas no subdiretório do Windows do diretório inicial.

Se esta política estiver desabilitada, 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 do 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 e atributos do objeto de usuário do Active Directory entre sinais de cerquilha.

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 do usuário no meio de uma sessão, antes do logoff.

Se esta política não for configurada aqui, o valor do arquivo .ini será usado. Se esta política não for configurada aqui ou no arquivo .ini, ela será ativada.

Suporte a perfis offline

Esta política permite que os perfis sejam sincronizados com o armazenamento do usuário na primeira oportunidade possível. Ela é destinada a usuários de laptop ou dispositivos móveis que se deslocam. Quando ocorre uma desconexão de rede, os perfis permanecem intactos no laptop ou dispositivo mesmo após a reinicialização ou hibernação. À medida que os usuários móveis trabalham, seus perfis são atualizados localmente e são eventualmente sincronizados com o armazenamento do usuário quando a conexão de rede é restabelecida.

Se esta política não for configurada aqui, o valor do arquivo .ini será usado. Se esta política não for configurada aqui ou no arquivo .ini, os perfis offline serão desativados.

Registro de gravação ativa de volta

Use esta política junto com "Gravação ativa de volta". As entradas de registro que são modificadas podem ser sincronizadas com o armazenamento do usuário no meio de uma sessão.

Se você não configurar esta configuração 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 desativado.

Suporte a perfis offline

Ativa o recurso de perfis offline. Este recurso é destinado a computadores que são comumente removidos de redes, tipicamente laptops ou dispositivos móveis, e não servidores ou desktops.

Se esta definição não for configurada aqui, o valor do arquivo .ini será usado.

Se esta definição 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 são desabilitadas. Ative o processamento habilitando esta política, mas somente após um planejamento e teste completos desse recurso.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

Grupos de usuários de configurações multiplataforma

Insira um ou mais grupos de usuários do Windows. Por exemplo, você pode usar esta política para processar apenas os perfis de um grupo de usuários de teste. Se esta política estiver configurada, o recurso de configurações multiplataforma do Profile Management processará apenas os membros desses grupos de usuários. Se esta política estiver desabilitada, o recurso processará todos os usuários especificados pela política de grupos processados.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, todos os grupos de usuários serão processados.

Caminho para definições multiplataforma

Identifica o local de rede dos arquivos de definição que você copiou do pacote de download. Este caminho deve ser um caminho UNC. Os usuários devem ter acesso de leitura a este local, e os administradores devem ter acesso de gravação a ele. O local deve ser um compartilhamento de arquivos Server Message Block (SMB) ou Common Internet File System (CIFS).

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

Caminho para o armazenamento de configurações multiplataforma

Define o caminho para o armazenamento de configurações multiplataforma, a pasta onde as configurações multiplataforma dos usuários são salvas. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial.

Esta área é a área comum do armazenamento de usuário onde os dados de perfil compartilhados por várias plataformas estão localizados. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial. Você pode usar as mesmas variáveis que para o **Caminho para o armazenamento de usuário**.

Se esta política estiver desabilitada, o caminho Windows\PM_CP será usado. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o valor padrão será usado.

Fonte para criar configurações entre plataformas

Especifica uma plataforma como a plataforma base se esta política estiver habilitada na UO dessa plataforma. Esta política migra dados dos perfis da plataforma base para o armazenamento de configurações entre plataformas.

Cada conjunto de perfis de cada plataforma é armazenado em uma UO separada. Você deve decidir quais dados de perfil da plataforma usar para preencher o armazenamento de configurações entre plataformas. É referida como a plataforma base. Se o armazenamento de configurações entre plataformas contiver um arquivo de definição sem dados, ou se os dados em cache em um perfil de plataforma única forem mais recentes do que os dados da definição no armazenamento, o Profile Management migrará os dados do perfil de plataforma única para o armazenamento, a menos que você desabilite esta política.

> **Importante:**
>
> Se esta política estiver habilitada em várias UOs, ou em vários objetos de usuário ou máquina, a plataforma na qual o primeiro usuário faz logon se torna o perfil base. Por padrão, esta política está Habilitada.

Configurações de política do sistema de arquivos

Configurações da política de exclusões

Esta seção descreve as configurações de política para configurar quais arquivos e diretórios no perfil de um usuário são excluídos do processo de sincronização.

LISTA DE EXCLUSÃO - ARQUIVOS

Lista de arquivos que são ignorados durante a sincronização. Os nomes dos arquivos devem ser caminhos relativos ao perfil do usuário (%USERPROFILE%). Curingas são suportados em nomes

de arquivos e em nomes de pastas, mas apenas curingas em nomes de arquivos são aplicados recursivamente.

Exemplos:

- `Desktop\Desktop.ini` ignora o arquivo `Desktop.ini` na pasta `Desktop`
- `%USERPROFILE%*.tmp` ignora todos os arquivos com a extensão `.tmp` em todo o perfil
- `AppData\Roaming\MyApp*.tmp` ignora todos os arquivos com a extensão `.tmp` em uma parte do perfil
- `Downloads*\a.txt` ignora `a.txt` em qualquer subpasta imediata da pasta `Downloads`.

Se esta política estiver desabilitada, nenhum arquivo será excluído. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhum arquivo será excluído.

HABILITAR LISTA DE EXCLUSÃO PADRÃO - DIRETÓRIOS

Lista padrão de diretórios ignorados durante a sincronização. Use esta política para especificar diretórios de exclusão de GPO sem 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 desabilitada, nenhuma pasta será excluída. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será excluída.

VERIFICAÇÃO DE EXCLUSÃO DE LOGON

Esta configuração define o que o Profile Management faz se um perfil no armazenamento do usuário contiver arquivos ou pastas excluídos.

Se esta configuração estiver desabilitada ou definida para o valor padrão de "Sincronizar arquivos ou pastas excluídos no logon", o Profile Management sincroniza arquivos ou pastas excluídos do armazenamento do usuário para o perfil local quando um usuário faz logon.

Se esta configuração estiver 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.

Se esta configuração estiver 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.

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, os arquivos ou pastas excluídos serão sincronizados do armazenamento do usuário para um perfil local quando um usuário fizer logon.

MANUSEIO DE ARQUIVOS GRANDES - ARQUIVOS A SEREM CRIADOS COMO LINKS SIMBÓLICOS

Para melhorar o desempenho do logon e processar arquivos grandes, o Profile Management cria um link simbólico em vez de copiar arquivos nesta lista.

Você pode usar curingas em políticas que se referem a arquivos; por exemplo, `!ctx_localappdata!\Microsoft\Outlook*.OST`.

Para processar o arquivo de pasta offline (`*.ost`) do Microsoft Outlook, certifique-se de que a pasta **Outlook** não esteja excluída para o Profile Management.

Esses arquivos não podem ser acessados em várias sessões simultaneamente.

Configurações da política de sincronização

A seção **Sincronização** descreve as configurações de política para especificar quais arquivos e pastas no perfil de um usuário são sincronizados entre o sistema onde o perfil está instalado e o armazenamento do usuário.

DIRETÓRIOS PARA SINCRONIZAR

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema onde está instalado e o armazenamento do 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, somente 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 do 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, somente 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 a outros.

Espelhar pastas permite que o Profile Management processe uma pasta transacional e seu conteúdo como uma única entidade, evitando o inchaço do perfil. Por exemplo, você pode

espelhar a pasta **cookies do Internet Explorer** para que o Index.dat seja sincronizado com os cookies que ele indexa. Nessas situações, a "última gravação vence". Assim, os arquivos em pastas espelhadas que foram modificados em mais de uma sessão são sobrescritos pela última atualização, resultando na perda de alterações do perfil.

Por exemplo, considere como o Index.dat referencia cookies enquanto um usuário navega na Internet. Se um usuário tiver duas sessões do Internet Explorer, cada uma em um servidor diferente, e visitar sites diferentes em cada sessão, os cookies de cada site serão adicionados ao servidor apropriado. Quando 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. No entanto, em vez disso, eles são mesclados, e as referências aos cookies no Index.dat ficam desatualizadas. A navegação posterior em novas sessões resulta em mesclagem repetida e uma pasta de cookies inchada.

Espelhar a pasta de cookies resolve o problema sobrescrevendo os cookies com os 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 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 especificado para pastas redirecionadas.

Por padrão, esta configuração está desabilitada e a variável de ambiente `%userdomain%` não é incluída como parte do caminho UNC especificado para pastas redirecionadas.

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 Documentos

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Documentos** para um local de rede compartilhado.

CAMINHO DE DOCUMENTOS

Esta configuração especifica o local de rede para o qual os arquivos na pasta **Documentos** são redirecionados.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

A configuração **Caminho de Documentos** deve ser habilitada não apenas para redirecionar arquivos para a pasta **Documentos**, mas também para redirecionar arquivos para as pastas **Música**, **Imagens** e **Vídeos**.

CONFIGURAÇÕES DE REDIRECIONAMENTO PARA DOCUMENTOS

Esta configuração especifica como redirecionar o conteúdo da pasta **Documentos**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Documentos**, escolha uma das seguintes opções:

- Redirecionar para o seguinte caminho UNC. Redireciona o conteúdo para o caminho UNC especificado na configuração de política Caminho de Documentos.
- Redirecionar para o diretório inicial do usuário. Redireciona o conteúdo para o diretório inicial do usuário, tipicamente configurado como o atributo #homeDirectory# para um usuário no Active Directory.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de Imagens

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Imagens** para um local de rede compartilhado.

CAMINHO DAS IMAGENS

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **Imagens** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redireciona a pasta especificada.

CONFIGURAÇÕES DE REDIRECIONAMENTO PARA IMAGENS

Esta configuração especifica como redirecionar o conteúdo da pasta **Imagens**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Imagens**, escolha uma das seguintes opções:

- Redirecionar para o seguinte caminho UNC. Redireciona o conteúdo para o caminho UNC especificado na configuração de política Caminho das Imagens.
- Redirecionar em relação à pasta Documentos. Redireciona o conteúdo para uma pasta relativa à pasta Documentos.

Para redirecionar o conteúdo para uma pasta relativa à pasta **Documentos**, a configuração **Caminho dos Documentos** deve estar habilitada.

Se esta configuração não for configurada aqui, o Profile Management não redireciona a pasta especificada.

Configurações de política de log

Esta seção contém configurações de política que configuram o log do Profile Management.

Ações do Active Directory

Essa configuração habilita ou desabilita o log detalhado das ações executadas no Active Directory.

Por padrão, essa configuração está desabilitada.

Ao habilitar essa configuração, certifique-se de que a configuração **Habilitar log** também esteja habilitada.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, erros e informações gerais serão registrados.

Informações comuns

Essa configuração habilita ou desabilita o log detalhado de informações comuns.

Por padrão, essa configuração está desabilitada.

Ao habilitar essa configuração, certifique-se de que a configuração **Habilitar log** também esteja habilitada.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, erros e informações gerais serão registrados.

Avisos comuns

Esta configuração habilita ou desabilita o registro detalhado de avisos comuns.

Por padrão, esta configuração está desativada.

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 aqui ou no arquivo .ini, erros e informações gerais serão registrados.

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 desativada 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, apenas erros serão registrados.

Ações do sistema de arquivos

Esta configuração habilita ou desabilita o registro detalhado de ações realizadas no sistema de arquivos.

Por padrão, esta configuração está desativada.

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 aqui ou no arquivo .ini, erros e informações gerais serão registrados.

Notificações do sistema de arquivos

Esta configuração habilita ou desabilita o registro detalhado de notificações do sistema de arquivos.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar log** 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, erros e informações gerais serão registrados.

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 log** 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, erros e informações gerais serão registrados.

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 configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, erros e informações gerais serão registrados.

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, isso 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) será excluído, o arquivo de log será renomeado para .bak e um novo arquivo de log será criado.

O arquivo de log é criado em `%SystemRoot%\System32\Logfiles\UserProfileManager`.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, o 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. Isso 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, mas a conta do sistema para as máquinas deve ter acesso de gravação ao compartilhamento UNC. Use um caminho local para quaisquer laptops gerenciados pelo recurso de perfis offline.

Se um caminho UNC for usado para arquivos de log, a Citrix recomenda que uma lista de controle de acesso apropriada seja aplicada à pasta de arquivos de log para garantir que apenas contas de usuário ou computador autorizadas possam acessar os arquivos armazenados.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, o local padrão %SystemRoot%\System32\Logfiles\UserProfileManager será usado.

Informações de usuário personalizadas

Esta configuração habilita ou desabilita o registro em log detalhado de informações de usuário personalizadas.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Enable logging** também esteja habilitada.

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, erros e informações gerais serão registrados.

Valores de política no logon e logoff

Esta configuração habilita ou desabilita o registro em log detalhado dos valores de política quando um usuário faz logon e logoff.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Enable logging** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, erros e informações gerais serão registrados.

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 definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, erros e informações gerais serão registrados.

Diferenças do Registro ao fazer logoff

Esta configuração ativa ou desativa o registro detalhado de quaisquer diferenças no registro quando um usuário faz 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 definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, erros e informações gerais serão registrados.

Configurações de política de tratamento de perfil

Esta seção contém 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 no final do processo de logoff. O Profile Management verifica os logoffs a cada minuto, então um valor de 60 garante que os perfis sejam excluídos entre um e dois minutos após os usuários fazerem logoff (dependendo 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, isso também pode acelerar o logoff.

Por padrão, isso é definido como 0 e o Profile Management exclui 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 configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada 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 configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, os perfis em cache não serão excluídos.

Tratamento de conflitos de perfil local

Esta configuração define como o Profile Management se comporta se um perfil de usuário existir tanto no armazenamento de usuário quanto como um perfil de usuário local do Windows (não 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 armazenamento 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 armazenamento de usuário.

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 locais existentes serão usados.

Migração de perfis existentes

Esta configuração especifica os tipos de perfil migrados para o armazenamento de usuário durante o logon se um usuário não tiver um perfil atual no armazenamento de usuário.

O Profile Management pode migrar perfis existentes "em tempo real" durante o logon se um usuário não tiver um perfil no armazenamento de usuário. Depois disso, o perfil do armazenamento de usuário é usado pelo Profile Management tanto na sessão atual quanto em qualquer outra sessão configurada com o caminho para o mesmo armazenamento de usuário.

Por padrão, perfis locais e perfis de roaming são migrados para o armazenamento de usuário durante o logon.

Para especificar os tipos de perfil migrados para o armazenamento de usuário durante o logon, escolha uma das seguintes opções:

- Perfis locais e de roaming
- Local
- Roaming
- Nenhum (Desativado)

Se você selecionar **Nenhum**, o sistema usará o mecanismo existente do Windows para criar perfis, como se estivesse em um ambiente onde o Profile Management não está instalado.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, os perfis locais e de roaming existentes serão migrados.

Migração automática de perfis de 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 do registro em `HKEY_CURRENT_USER\SOFTWARE`. Esta configuração pode ser útil em casos em que 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 aplicativos 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 do 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 curto do SO incluindo a variável "!CTX_OSNAME!" no caminho do armazenamento do usuário. Isso permite que o Profile Management localize os perfis de aplicativos existentes.

Se esta configuração não for definida aqui, a configuração do arquivo .ini será usada.

Se esta configuração não for definida aqui ou no arquivo .ini, ela será desabilitada por padrão.

Caminho para o perfil de modelo

Esta configuração especifica o caminho para o perfil que você deseja que o Profile Management use como modelo para criar perfis de usuário.

O caminho especificado deve ser o caminho completo para a pasta que contém o arquivo de registro NTUSER.DAT e quaisquer outras pastas e arquivos necessários para o perfil de modelo.

Nota: Não inclua NTUSER.DAT no caminho. Por exemplo, com o arquivo `\\myservername\myprofiles\template\ntuser.dat`, defina o local como `\\myservername\myprofiles\template`.

Use caminhos absolutos, que podem ser caminhos UNC ou caminhos na máquina local. Use este último, por exemplo, para especificar um perfil de modelo permanentemente em uma imagem do Citrix Provisioning™ Services. Caminhos relativos não são suportados.

Nota: Esta configuração não oferece suporte à expansão de atributos do Active Directory, variáveis de ambiente do sistema ou as variáveis `%USERNAME%` e `%USERDOMAIN%`.

Por padrão, esta configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo substitui perfil local

Esta configuração permite que o perfil de modelo substitua o perfil local ao criar perfis de usuário.

Se um usuário não tiver um perfil de usuário Citrix, mas um perfil de usuário local do Windows existir, por padrão o perfil local será usado (e migrado para o armazenamento de usuário, se isso não estiver desabilitado). Habilitar esta configuração de política permite que o perfil de modelo substitua o perfil local usado ao criar perfis de usuário.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo substitui perfil móvel

Esta configuração permite que o perfil de modelo substitua um perfil móvel ao criar perfis de usuário.

Se um usuário não tiver um perfil de usuário Citrix, mas existir um perfil de usuário móvel do Windows, por padrão o perfil móvel será usado (e migrado para o armazenamento de usuário, se isso não estiver desabilitado). Habilitar esta configuração de política permite que o perfil de modelo substitua o perfil móvel usado ao criar perfis de usuário.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo usado como um perfil obrigatório Citrix para todos os logons

Esta configuração permite que o Profile Management use o perfil de modelo como o perfil padrão para criar todos os perfis de usuário.

Por padrão, esta configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

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). Essa solução reduz os tempos de logon mapeando as pastas especificadas para o disco de perfil que é armazenado na rede. O contêiner de perfil anexa o disco de perfil contendo essas pastas durante o logon, eliminando assim a necessidade de salvar uma cópia das pastas no perfil local. Isso diminui os tempos de logon.

Habilitar cache local para contêineres de perfil

Esta política habilita o suporte a cache local para contêineres de perfil do Citrix Profile Management. Com a política definida como **Habilitado**, cada perfil local serve como um cache

local de seu contêiner de perfil do Citrix Profile Management. Se o streaming de perfil estiver em uso, os arquivos armazenados em cache localmente são criados sob demanda. Caso contrário, eles são criados durante os logons do usuário. Para usar o recurso de cache local, coloque um perfil de usuário inteiro em seu contêiner de perfil do Citrix Profile Management.

Pastas a serem excluídas do contêiner de perfil

Lista de pastas a serem excluídas de um contêiner de perfil do Citrix Profile Management.

Pastas a serem incluídas no contêiner de perfil

Lista de pastas a serem mantidas em um contêiner de perfil do Citrix Profile Management quando suas pastas pai são excluídas.

As pastas nesta lista devem ser subpastas das pastas excluídas. Caso contrário, esta configuração não funciona.

Arquivos a serem incluídos no contêiner de perfil

Lista de arquivos a serem incluídos em um contêiner de perfil do Citrix Profile Management.

Os arquivos nesta lista devem estar dentro das pastas excluídas. Caso contrário, esta configuração não funciona.

Arquivos a serem excluídos do contêiner de perfil

Lista de arquivos a serem excluídos de um contêiner de perfil do Citrix Profile Management.

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, aprimorando a experiência do usuário.

Use esta configuração com a configuração **Transmissão 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 aqui ou 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 todos os arquivos desse 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 inteiro é usado. Quando o recurso de cache de perfil inteiro 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 aqui ou no arquivo .ini, ela será desabilitada.

Transmissão de perfil

Esta configuração habilita e desabilita o recurso de perfis de usuário transmitidos do Citrix®. Quando habilitado, arquivos e pastas contidos em um perfil são buscados do armazenamento do usuário para o computador local somente quando acessados pelos usuários após o logon. Entradas de registro e arquivos na área pendente são buscados imediatamente.

Por padrão, o streaming de perfil está desativado.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, ela será desativada.

Grupos de perfis de usuário transmitidos

Esta configuração especifica quais perfis de usuário dentro de uma UO 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 UO são processados normalmente.

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, todos os perfis de usuário serão processados.

Para ativar a exclusão de streaming de perfil

Quando a exclusão de streaming de perfil está ativada, o Profile Management não transmite pastas na lista de exclusão, e 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 do usuário a partir da área pendente, caso o armazenamento do usuário permaneça bloqueado quando um servidor se tornar sem resposta. Isso evita o inchaço na área pendente e garante que o armazenamento do usuário sempre contenha os arquivos mais atualizados.

Por padrão, isso é definido como 1 (um) dia.

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.

Configurações de política da camada de personalização do usuário

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, use parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- O tamanho máximo que quaisquer novos discos de camada de usuário podem atingir.

Para fazer isso, estas duas políticas aparecem na lista de políticas disponíveis:

- User Layer Repository Path - Insira um caminho no formato ‘\\nome do servidor ou endereço\nome da pasta’ no campo Valor.
- User Layer Size GB - O tamanho padrão da camada de usuário de 10 GB é o mínimo que recomendamos. Uma camada de usuário é um disco de provisionamento dinâmico que se expande até o tamanho definido à medida que o espaço é usado. As camadas de usuário nunca diminuem de tamanho.

> **Observação:**

> Aumentar o tamanho da Camada de Usuário afeta novas camadas de usuário e expande as existentes. Diminuir o tamanho da camada afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

> Para obter mais informações, consulte Camada de personalização do usuário.

Configurações de política do Virtual Delivery Agent

A seção Virtual Delivery Agent (VDA) contém configurações de política que controlam a comunicação entre o VDA e os controladores de um site.

Importante: O VDA requer as 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

Essa configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial (em vez de um IP global, se um estiver registrado). Essa configuração especifica o endereço IPv6 e a rede onde o VDA será registrado. O VDA se registrará apenas no primeiro endereço que corresponder à máscara de rede especificada. Essa configuração é válida apenas se a configuração de política Usar apenas registro de controlador IPv6 estiver habilitada.

Por padrão, esta configuração está em branco.

Porta de registro do Controller

Use esta configuração apenas se a configuração Ativar atualização automática de controladores estiver desativada.

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 é uma configuração opcional que pode ser usada com a configuração Controllers para restringir a lista de Controllers usados para registro.

Por padrão, esta configuração está em branco.

Controllers

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 é uma configuração opcional que pode ser usada com a configuração SIDs do Controller.

Por padrão, esta configuração está em branco.

Habilitar atualização automática de controllers

Esta configuração permite que o VDA se registre em um Controller automaticamente após a instalação.

Após o registro do VDA, o Controller no qual ele se registrou envia uma lista dos FQDNs e SIDs atuais do controller para o VDA. O VDA grava essa lista no armazenamento persistente. Cada Controller também verifica o banco de dados do Site a cada 90 minutos para obter informações do Controller; se um Controller foi adicionado ou removido desde a última verificação, ou se uma alteração de política ocorreu, o Controller envia listas atualizadas para seus VDAs registrados. O VDA aceitará conexões de todos os Controllers na lista mais recente que recebeu.

Por padrão, esta configuração está habilitada.

Usar apenas registro de controller IPv6

Esta configuração controla qual forma de endereço o VDA usa para se registrar no Controller:

- Quando ativado, o VDA se registra com o 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 Habilitar atualização automática de controladores estiver desativada.

Esta configuração especifica o Identificador Globalmente Único (GUID) do site que o VDA usa para se registrar com 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 contém configurações de política para habilitar e configurar a ferramenta de configuração de qualidade de imagem para os usuários. A ferramenta permite que os usuários otimizem o uso da largura de banda disponível ajustando em tempo real o equilíbrio entre a qualidade da imagem e a capacidade de resposta.

Habilitar sem perdas

Esta 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.

Quando um usuário habilita a compactação sem perdas, a qualidade da imagem é automaticamente definida para o valor máximo disponível na ferramenta de configuração de imagem. Por padrão, a compactação baseada em GPU ou CPU pode ser usada, de acordo com os recursos do dispositivo do usuário e do computador host.

Configurações de qualidade do HDX 3D Pro

Esta configuração especifica os valores mínimo e máximo que definem o intervalo de ajuste da qualidade da imagem disponível para os usuários 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 contém configurações de política para monitoramento de processos, recursos e falhas de aplicativos.

O escopo dessas políticas pode ser definido com base no Site, grupo de entrega, tipo de grupo de entrega, unidade organizacional e 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. Se você não quiser monitorar dados de recursos ou dados de processos, ou ambos, para um escopo específico (por exemplo, um grupo de entrega ou unidade organizacional específica), é recomendável desabilitar a política.

HABILITAR MONITORAMENTO DE PROCESSOS

Habilite esta configuração para permitir o monitoramento de processos em execução em máquinas com VDAs. Estatísticas como uso de CPU e memória são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificações em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Desabilitado.

HABILITAR MONITORAMENTO DE RECURSOS

Habilite esta configuração para permitir o monitoramento de contadores de desempenho críticos em máquinas com VDAs. Estatísticas (como uso de CPU e memória, IOPS e dados de latência de disco) são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificação em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Habilitado.

ESCALABILIDADE

Os dados de CPU e memória são enviados para o banco de dados de cada VDA em intervalos de 5 minutos. Os dados de processo (se habilitados) 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 **habilitados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados de 5 Minutos	1 Dia
Dados de 10 Minutos	7 Dias
Dados Horários	30 Dias
Dados Diários	90 Dias

DADOS DE IOPS E LATÊNCIA DE DISCO

Os dados de IOPS e latência de disco estão **Habilitados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados Horários	3 Dias
Dados Diários	90 Dias

Com as configurações de retenção de dados, aproximadamente 276 KB de espaço em disco são necessários para armazenar os dados de CPU, memória, IOPS e latência de disco para um VDA durante um período de um ano.

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO
1	276 KB
1K	270 MB

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO
40K	10.6 GB

DADOS DE PROCESSO

Os dados de processo estão **Desabilitados** por padrão. Recomenda-se habilitar os dados de processo em um subconjunto de máquinas conforme a necessidade. As configurações padrão de retenção de dados para os dados de processo são as seguintes:

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados de 10 minutos	1 Dia
Dados por Hora	7 Dias

Se os dados de processo estiverem habilitados com as configurações de retenção padrão, os dados de processo consumiriam aproximadamente 1,5 MB por VDA e 3 MB por VDA de Serviços de Terminal (TS VDA) durante um período de um ano.

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA VDA	ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA TS VDA
1	1,5 MB	3 MB
1K	1,5 GB	3 GB

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, isso consome armazenamento extra. Ao habilitar as configurações abaixo, você pode obter mais precisão nos dados de utilização do processo. As configurações que podem ser habilitadas são:

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

Essas configurações podem ser habilitadas a partir do cmdlet do PowerShell de Monitoramento: Set-MonitorConfiguration

Políticas para monitoramento de falhas de aplicativos

A guia **Falha de Aplicativo**, por padrão, exibe apenas falhas de aplicativos de VDAs de SO multi-sessão. As configurações de monitoramento de falha de aplicativo podem ser modificadas com as seguintes políticas de Monitoramento:

HABILITAR MONITORAMENTO DE FALHAS DE APLICATIVOS

Use esta configuração para configurar o monitoramento de falhas de aplicativos para monitorar erros ou falhas de aplicativos (travamentos e exceções não tratadas), ou ambos. Desabilite o monitoramento de falhas de aplicativos definindo o **Valor** como **Nenhum**. O padrão para esta configuração é apenas falhas de aplicativos.

HABILITAR MONITORAMENTO DE FALHAS DE APLICATIVOS EM VDAS DE SO DE SESSÃO ÚNICA

Por padrão, apenas as falhas de aplicativos hospedados em VDAs de SO multi-sessão 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 Performance Analytics

COLETA DE DADOS DE VDA PARA ANÁLISE DE DESEMPENHO

Use a política para habilitar ou desabilitar o serviço Monitor de coletar métricas relacionadas ao desempenho dos VDAs para Análise de Desempenho. Por padrão, a política é **Permitido**. Defina a política como **Proibido** para interromper a coleta de dados dos VDAs.

Dicas de planejamento de armazenamento

Política de grupo. Se você não estiver interessado em monitorar os Dados de Recurso ou Dados de Processo, um ou ambos podem ser desativados usando a política de grupo. Para obter mais informações, consulte a seção Política de Grupo de Criar políticas.

Limpeza de dados. As configurações padrão de retenção de dados podem ser modificadas para limpar os dados mais cedo e liberar espaço de armazenamento. Para obter mais informações

sobre as configurações de limpeza, consulte Granularidade e retenção de dados em Acessando dados usando a API.

Configurar as configurações de Redirecionamento de Porta COM e Porta LPT usando o registro

Nas versões do VDA 7.0 a 7.8, as configurações de Porta COM e Porta LPT são configuráveis apenas usando o registro. Para versões do VDA anteriores a 7.0 e para versões do VDA 7.9 e posteriores, essas configurações são configuráveis no Studio. Para obter mais informações, consulte Configurações de política de redirecionamento de porta e Configurações de política de largura de banda.

As configurações de política para Redirecionamento de Porta COM e Porta LPT estão localizadas em HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated na imagem ou máquina VDA.

Para habilitar o redirecionamento de porta COM e porta LPT, adicione novas chaves de registro do tipo REG_DWORD, da seguinte forma:

Cuidado: Editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua 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
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

CHAVE DO REGISTRO	DESCRIÇÃO	VALORES PERMITIDOS
AutoConnectClientComPorts	Conectar automaticamente as portas COM do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)
AllowLptPortRedirection	Permitir ou proibir o redirecionamento de porta LPT	1 (Permitir) ou 0 (Proibir)
LimitLptBw	Limite de largura de banda para o canal de redirecionamento de porta LPT	Valor numérico
LimitLptBwPercent	Limite de largura de banda para o canal de redirecionamento de porta LPT como uma porcentagem da largura de banda total da sessão	Valor numérico entre 0 e 100
AutoConnectClientLptPorts	Conectar automaticamente portas LPT do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)

Após configurar essas definições, altere seus catálogos de máquinas para usar a nova imagem mestre ou máquina física atualizada. Os desktops são atualizados com as novas definições na próxima vez que os usuários fizerem logoff.

Configurações de política do Connector para Configuration Manager 2012

A seção Connector para Configuration Manager 2012 contém configurações de política para configurar o agente Citrix Connector 7.5.

> **Importante:**

> As políticas de mensagem de aviso, logoff e reinicialização se aplicam 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 Studio para notificar os usuários. Para catálogos de SO de sessão única gerenciados manualmente, use o Configuration Manager para notificar os usuários. Para catálogos de SO de sessão única gerenciados por Provisioning Services, use o Provisioning Services para notificar os usuários.

Intervalo de frequência de aviso

Essa configuração define o intervalo entre as aparições da mensagem de aviso aos usuários.

Os intervalos são definidos usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração 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 aos usuários, notificando-os sobre as próximas atualizações de software ou manutenção que exige que eles façam logoff.

Por padrão, a mensagem é: {TIMESTAMP} Salve seu trabalho. O servidor ficará offline para manutenção em {TIMELEFT}.

Título da caixa de mensagem de aviso

Esta configuração contém o texto editável da barra de título da mensagem de aviso aos usuários.

Por padrão, o título é: Manutenção Programada

Período de tempo do aviso

Esta configuração define quanto tempo antes da manutenção a mensagem de aviso aparece pela primeira vez.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.

- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração é de 16 horas (16:00:00), indicando que a primeira mensagem de aviso aparece aproximadamente 16 horas antes da manutenção.

Texto do corpo da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da mensagem que alerta os usuários de que um logoff forçado foi iniciado.

Por padrão, a mensagem é: O servidor está atualmente ficando offline para manutenção

Título da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da barra de título da mensagem final de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

Período de carência para logoff forçado

Esta configuração define o período de tempo entre a notificação aos usuários para fazer logoff e a implementação do logoff forçado para processar a manutenção pendente.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0–999.
- hh são horas com um intervalo de 0–23.
- mm são minutos com um intervalo de 0–59.
- ss são segundos com um intervalo de 0–59.

Por padrão, a configuração do período de carência para logoff forçado é de 5 minutos (00:05:00).

Texto do corpo da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da mensagem que informa aos usuários para salvar seu trabalho e fazer logoff antes do início de um logoff forçado.

Por padrão, a mensagem contém o seguinte: {TIMESTAMP} Salve seu trabalho e faça logoff. O servidor ficará offline para manutenção em {TIMELEFT}.

Título da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da barra de título da mensagem de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

Modo gerenciado por imagem

O agente do Connector detecta automaticamente se está sendo executado em um clone de máquina gerenciado pelo Provisioning Services ou MCS. O agente bloqueia as atualizações do Configuration Manager em clones gerenciados por imagem e instala automaticamente as atualizações na imagem mestre do catálogo.

Após a atualização de uma imagem mestre, use o Studio para orquestrar a reinicialização dos clones do catálogo MCS. O Agente do Connector orquestra automaticamente a reinicialização dos clones do catálogo PVS durante as janelas de manutenção do Configuration Manager. Para substituir esse comportamento, de modo que o software seja instalado em clones de catálogo pelo Configuration Manager, altere o Modo gerenciado por imagem para Desabilitado.

Texto do corpo da caixa de mensagem de reinicialização

Esta 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).

Gerenciar

Gerenciar um site Citrix Virtual Apps and Desktops™ abrange vários itens e tarefas.

Licenciamento

É necessária uma conexão válida com o Citrix License Server ao criar um site. Posteriormente, você pode concluir várias tarefas de licenciamento no Studio, incluindo adicionar licenças, alterar tipos ou modelos de licença e gerenciar administradores de licença. Você também pode acessar o Console de Administração de Licenças 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 Controllers, catálogos de máquinas e conexões de host estão em uma zona primária. Posteriormente, você pode usar o Studio para criar zonas satélites contendo esses itens. Depois que seu site tiver mais de uma zona, você poderá indicar em qual zona quaisquer catálogos de máquinas, conexões de host ou Controllers adicionados recém-criados serão colocados. Você também pode mover itens entre zonas.

Conexões e recursos

Se você estiver usando um hipervisor ou outro serviço para hospedar máquinas que fornecem aplicativos e desktops aos usuários, você cria sua primeira conexão com esse hipervisor ou outro serviço ao criar um site. Os detalhes de armazenamento e rede para essa conexão formam seus recursos. Posteriormente, você pode alterar essa conexão e seus recursos, e criar mais conexões. Você também pode gerenciar as máquinas que usam uma conexão configurada.

Cache de Host Local

O Cache de Host Local permite que as operações de intermediação de conexão em um site continuem quando a conexão entre um Delivery Controller™ e o banco de dados do site falha.

IP virtual e loopback virtual

O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem de comunicações com o localhost para usar um endereço de loopback virtual exclusivo no intervalo do localhost.

Controladores de Entrega

Este artigo contém considerações e procedimentos ao adicionar e remover Controllers de um site. Ele também descreve como mover Controllers para outra zona ou site, e como mover um VDA para outro site.

Registro de VDA com Controllers

Antes que um VDA possa ajudar a entregar aplicativos e desktops, ele deve se registrar (estabelecer comunicação) com um Controller. Os endereços do Controller podem ser especificados de várias maneiras, que são descritas neste artigo. É fundamental que os VDAs tenham informações atualizadas à medida que os Controllers são adicionados, movidos e removidos no site.

Sessões

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência do usuário. Vários recursos podem otimizar a confiabilidade das sessões, reduzir inconveniências, 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 somente a itens com uma tag específica.

IPv4/IPv6

O Citrix Virtual Apps and Desktops suporta 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 de 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 do Citrix. Ele foi feito para solucionar problemas complexos relacionados ao Citrix, analisar o suporte a filtros e coletar dados de desempenho.

Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios.

Citrix Scout

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manutenção proativa em sua implantação do Citrix Virtual Apps and Desktops. A Citrix oferece análise abrangente e automatizada de coleções de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

Licenciamento para Citrix Virtual Apps and Desktops™ usando o Studio

No Studio, você pode gerenciar e rastrear o licenciamento, se o servidor de licenças estiver no mesmo domínio do Studio ou em um domínio confiável. Para obter informações sobre tarefas de licenciamento, consulte a documentação de licenciamento e Licenciamento de vários tipos.

O Serviço de Ativação de Licenças (LAS) é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa ao licenciamento herdado 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.

A tabela a seguir lista as edições e os modelos de licença suportados:

PRODUTOS	EDIÇÕES	MODELOS DE LICENÇA
Citrix Virtual Apps™	Premium, Advanced, Standard	Concorrente
Citrix Virtual Desktops	Premium, Advanced, Standard	Usuário/Dispositivo e Concorrente

Para obter mais informações, consulte Licença concorrente e Licença de usuário/dispositivo.

Versão compatível do Current Release (CRs) e Long Term Service Release (LTSRs)

Para obter informações sobre as versões compatíveis de Current Release (CRs), Long Term Service Release (LTSRs) e versões mínimas compatíveis do LS, consulte a documentação Citrix Virtual Apps and Desktops current release.

> **Importante:**

> 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.

> Você deve ser um administrador de licenças completo para concluir as seguintes tarefas. Para visualizar informações de licença no 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 Studio

1. Selecione **Configuração \> Licenciamento** no painel de navegação do Studio.
2. Selecione **Alocar Licenças** no painel 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 de Licença específico, você não poderá reutilizar esse Código de Acesso de Licença. Para fazer outras transações com o mesmo código, faça login em Minha Conta.

Adicionar licenças armazenadas no seu computador local ou na rede

1. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione **Adicionar Licenças** no painel Ações.
3. Procure um arquivo de licença e adicione-o ao servidor de licenças.

Alterar o servidor de licenças

1. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione **Alterar Servidor de Licenças** no painel Ações.
3. Digite o endereço do servidor de licenças no formato *nome:porta*, onde o nome é um endereço DNS, NetBIOS ou IP. Se você não especificar um número de porta, a porta padrão (27000) será usada.

Selecione o tipo de licença a ser usado

- Ao configurar o Site, depois de especificar o servidor de licenças, você será solicitado a selecionar o tipo de licença a ser usado. Se não houver licenças no servidor, a opção de usar o produto por um período de 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 depois selecioná-lo.

Alterar a edição do produto e o modelo de licenciamento

1. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione **Editar Edição do Produto** no painel Ações.
3. Atualize as opções apropriadas.

Para acessar o Console de Administração de Licenças, no painel **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 Citrix 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. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione a guia Administradores de Licenciamento no painel central.
3. Selecione **Adicionar administrador de licenciamento** no painel 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. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione a guia Administradores de Licenciamento no painel central e, em seguida, selecione o administrador.
3. Selecione **Editar administrador de licenciamento** ou **Excluir administrador de licenciamento** no painel Ações.

Adicionar um grupo de administradores de licenciamento

1. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione a guia Administradores de Licenciamento no painel central.
3. Selecione **Adicionar grupo de administradores de licenciamento** no painel 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. Selecione **Configuração > Licenciamento** no painel de navegação do Studio.
2. Selecione a guia Administradores de Licenciamento no painel central e, em seguida, selecione o grupo de administradores.
3. Selecione **Editar grupo de administradores de licenciamento** ou **Excluir grupo de administradores de licenciamento** no painel Ações.

Exibir informações de licença

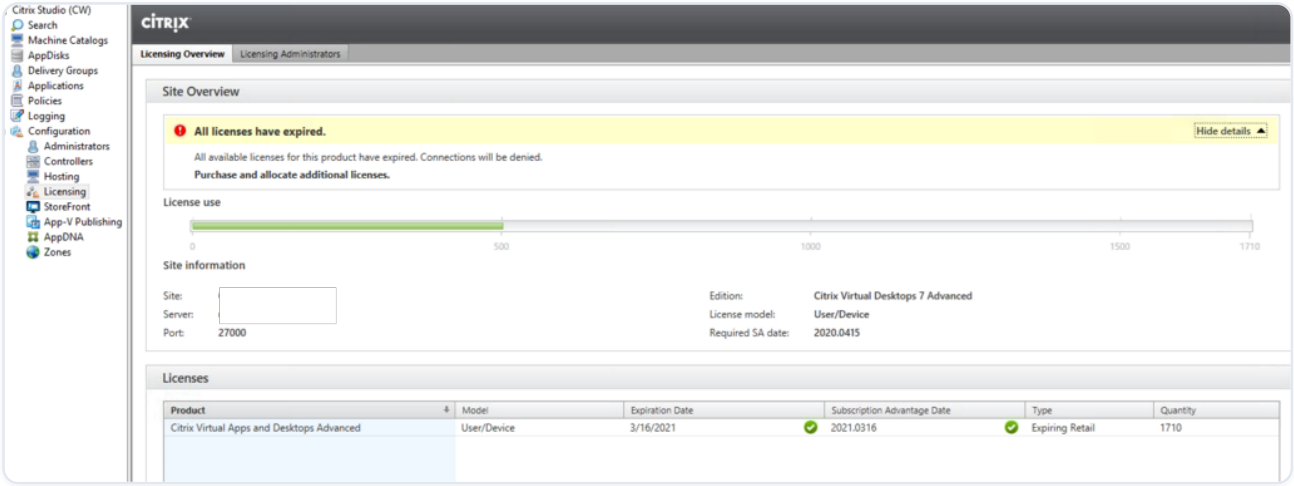
Selecione **Configuração > Licenciamento** no painel de navegação do Studio. Um resumo do uso e das configurações da licença para o Site é exibido com uma lista de todas as licenças atualmente instaladas no servidor de licenças especificado.

Certifique-se de que as configurações de licenciamento do site, que incluem o tipo de produto, edição da licença e modelo de licenciamento, correspondam às licenças que seu License Server configurado usa. Caso contrário, talvez seja necessário baixar ou alocar suas licenças existentes para corresponder às configurações de licença do site.

Visualizar alertas de expiração de licença

O Citrix Studio consulta as datas de expiração dos arquivos de licença no Citrix License Server. Os administradores são alertados se os arquivos de licença estiverem próximos da expiração ou já tiverem expirado.

Você pode ver os alertas na interface do usuário do Studio. A imagem a seguir mostra um alerta de expiração de licença exibido na UI do Citrix Studio.



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 tradicional herdado 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 servidor de licenças. Você só precisa atualizar seu servidor de licenças e se registrar no Citrix Cloud. Uma vez que os produtos compatíveis são apontados para o servidor de licenças, eles podem ser ativados automaticamente.

Após a ativação, o Servidor de Licenças 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 Servidor de Licenças ou o LAS estiverem inacessíveis, o sistema entra no modo de cache de licenças, que é 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 Servidor de Licenças para a versão 11.17.2 build 53100 ou posterior.
- Conexão de internet confiável e contínua para o Servidor de Licenças.
- As configurações de licença no nível do Grupo de Desktop devem ser desabilitadas.

> **Observação:**

> Para garantir que o licenciamento no nível do DG esteja desabilitado, use Get-brokerdesktopgroup e LicenseModel deve ser "None".

> **Observação:**

> Instale o .NET Framework 4.8 no Delivery Controller antes de iniciar a atualização para 2203 LTSR CU7. Isso garante que as ferramentas de Verificação de Compatibilidade de Licenciamento sejam executadas corretamente e evita avisos de licenciamento falsos.

Considerações

- Todos os Delivery Controllers devem ser compatíveis com o LAS antes que o Citrix Studio solicite a ativação. Um único site de controlador pode usar licenças herdadas ou LAS.
- Você pode ter vários Servidores de Licenças registrados com o mesmo ID do Citrix Cloud (CCID) ou OrgID. No entanto, um site pode ser configurado para apontar para apenas um servidor de licenças.

Limitações

- A migração para o 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 herdada existente para o LAS usando apenas o Citrix Studio.

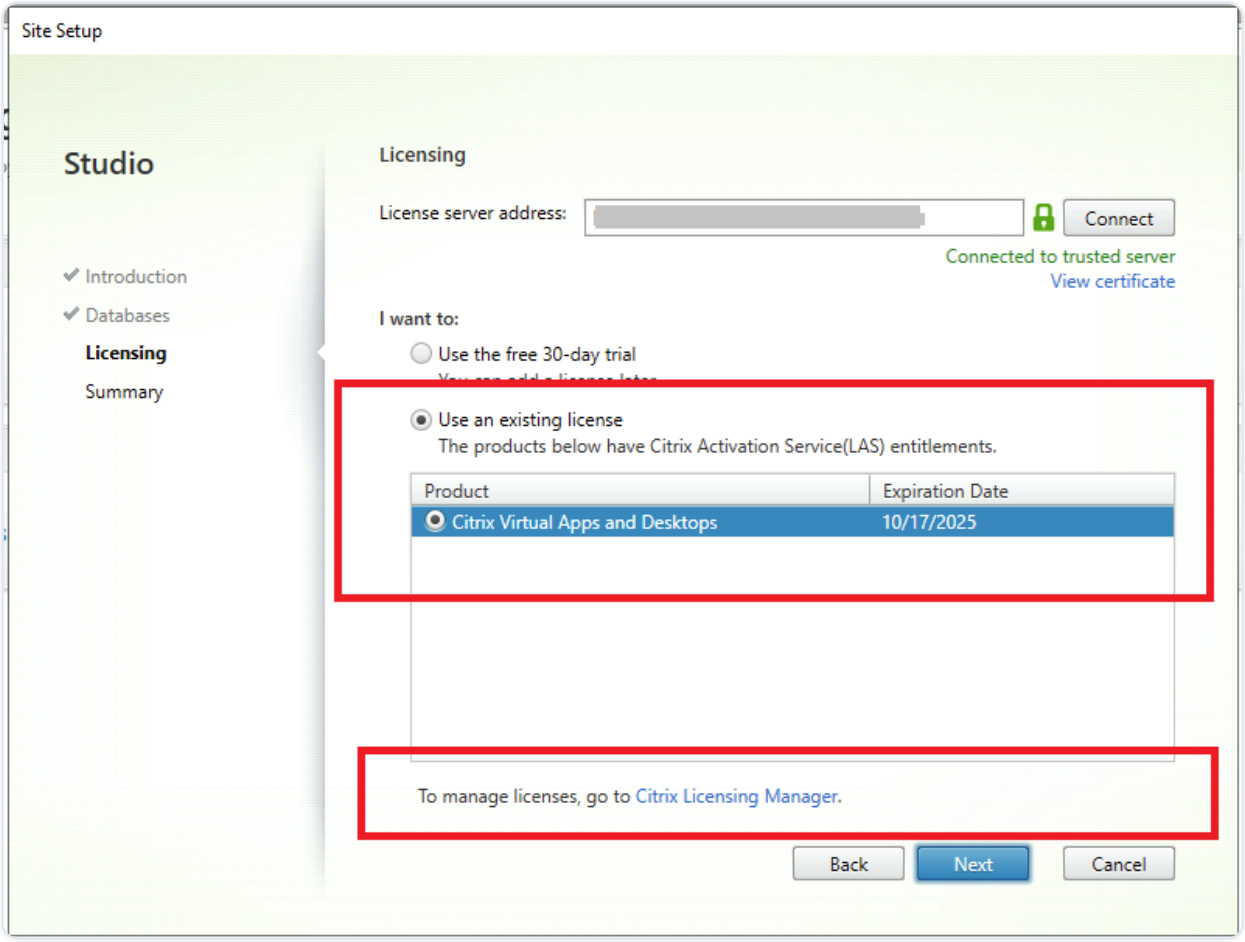
Etapas principais

1. Instale ou atualize o Servidor de Licenças para a versão 11.17.2 build 53100 ou posterior e configure o LAS conforme as instruções mencionadas em Como configurar o Servidor de Licenças para o Serviço de Ativação de Licenças.
2. Instale o Citrix Virtual Apps and Desktops versão 2203 LTSR CU7 ou posterior. Instale os componentes principais, como Citrix Delivery Controller, Citrix Studio e Citrix Director.

   > **Observação:**
   >
   > Todos os Delivery Controllers no site do Citrix Virtual Apps and Desktops devem ser compatíveis com o LAS.

3. Depois de instalar os componentes necessários, use o Citrix Studio 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:

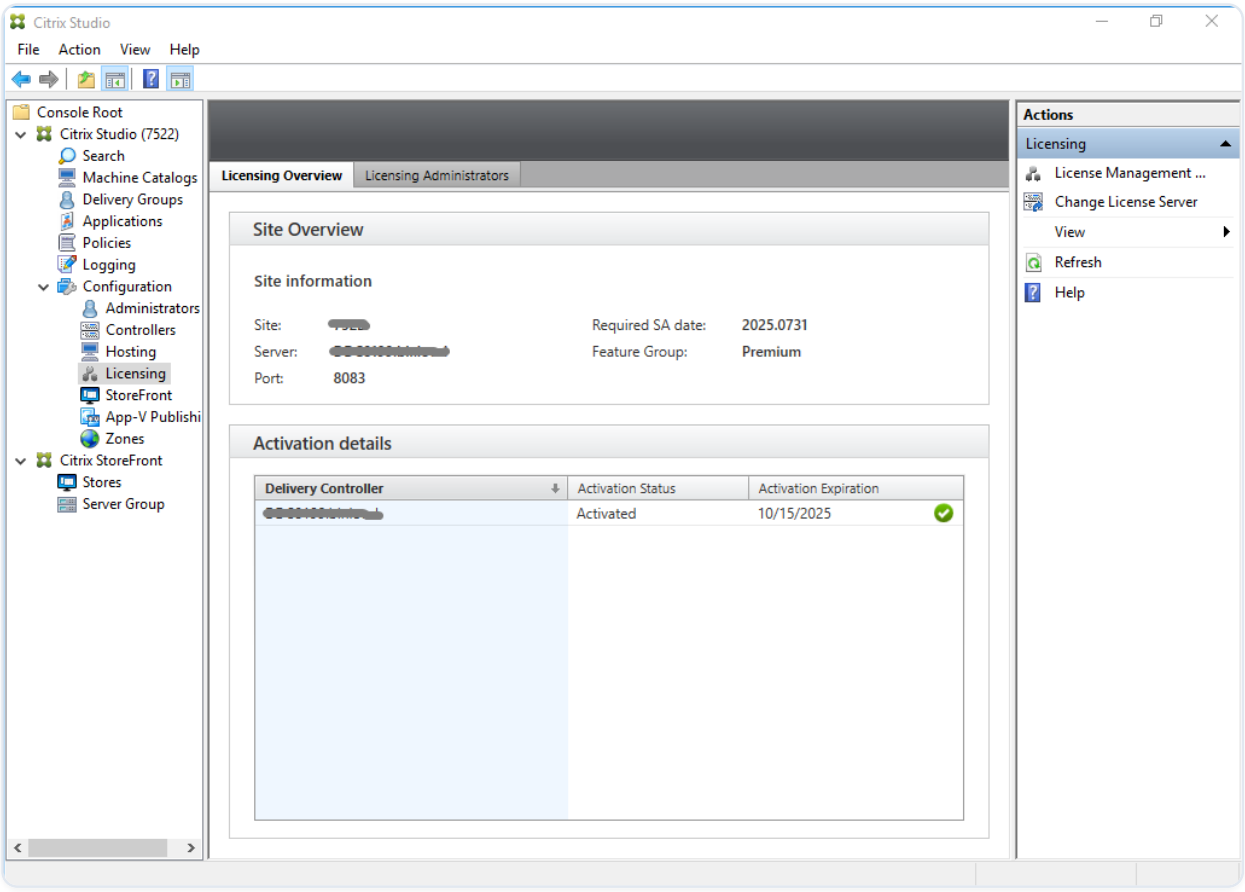
Se o License Server não for atualizado para a versão 53100 ou posterior, você encontrará erros de licenciamento. Ignorar esses erros e prosseguir com a atualização do site CVAD resultará na inoperabilidade do site.

4. Verificar detalhes de licenciamento.
5. Migrar licenciamento herdado para LAS.

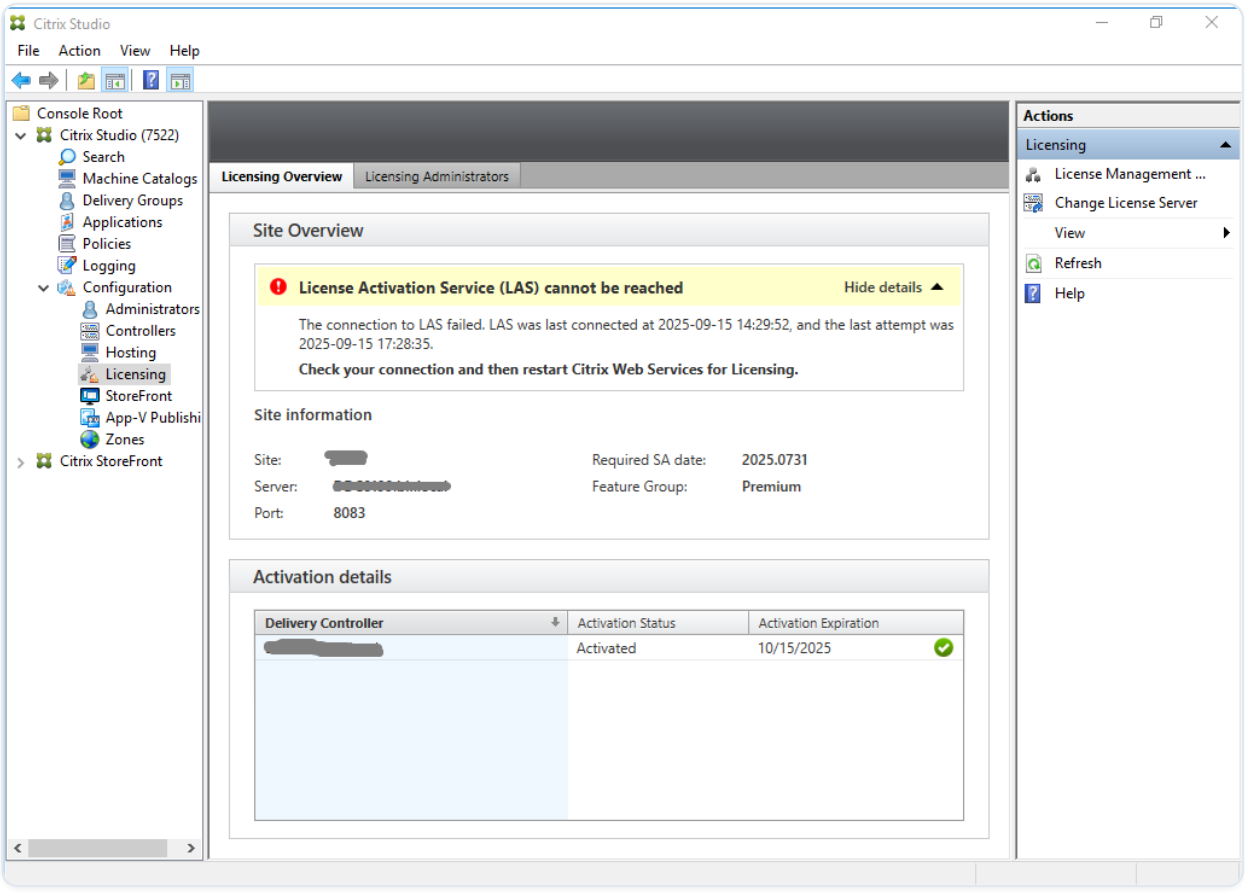
Verificar detalhes de licenciamento

Após criar o site, verifique os detalhes de licenciamento usando o Citrix Studio.

1. No Citrix Studio, selecione o nó **Licenciamento**.
2. Na página **Visão geral do licenciamento**, verifique se o site do Citrix Virtual Apps and Desktops possui a licença apropriada ou se a licença expirou ao usar os recursos do LAS.



Se o LAS não estiver acessível, você poderá ver uma mensagem de erro:



Se o seu License Server ainda estiver usando uma licença herdada antiga e o site do Citrix Virtual Apps and Desktops for compatível com LAS, o Citrix Studio solicitará que você registre seu License Server no Citrix Cloud.

Registrar o Servidor de Licenças para usar o LAS(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/register-license-server.png)

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:**
   - Depois que as etapas anteriores forem concluídas, clique em **Migrar para LAS**.

     Migrar de licença herdada para LAS(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/migrate-to-las.png)
   - 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 do LAS para o licenciamento legado

Faça o seguinte para reverter do LAS para o licenciamento legado:

1. Execute o seguinte comando PowerShell.

```
Set-ConfigSite -UseLicenseActivationService $false
```

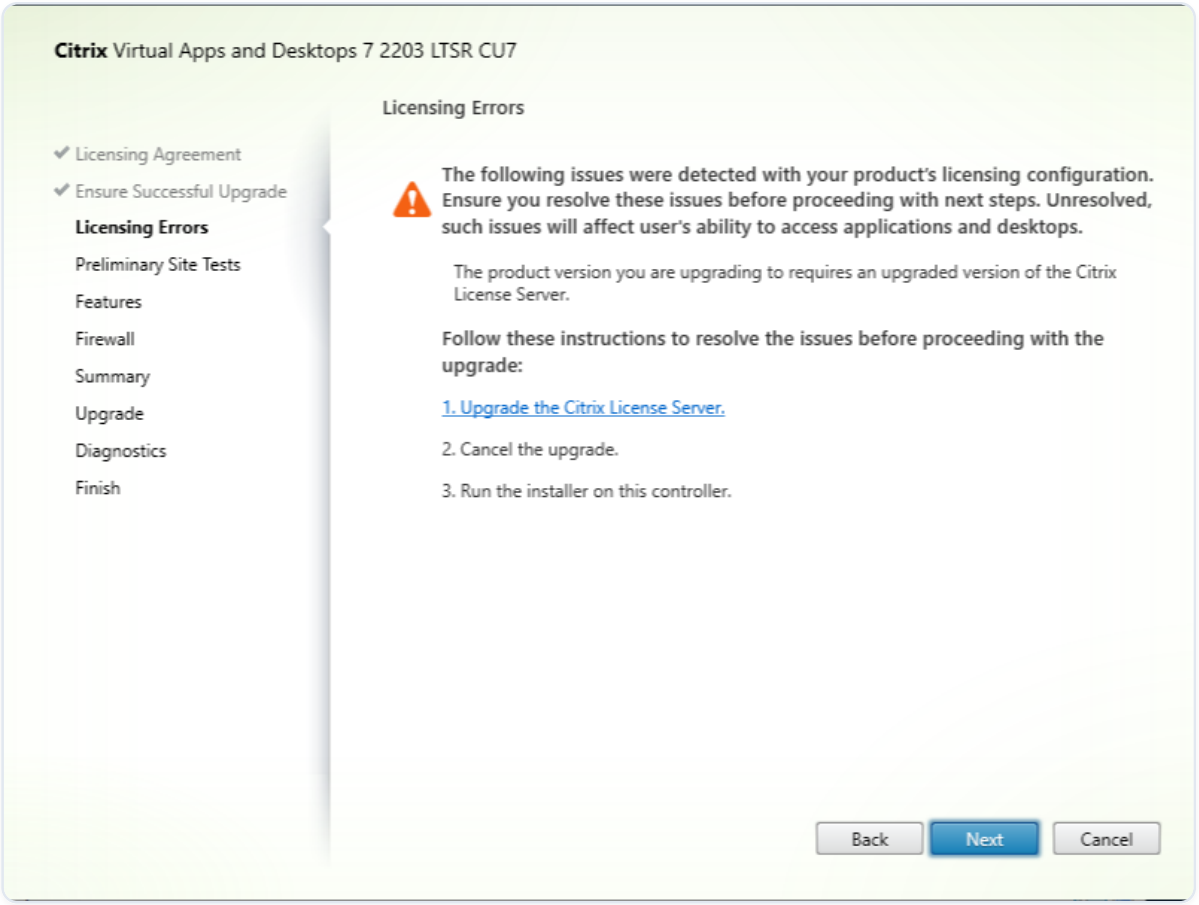
2. Configure as licenças legadas no Citrix Studio.

> **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 migrar para o Serviço de Ativação de Licenças (LAS). Para obter detalhes, consulte o anúncio.

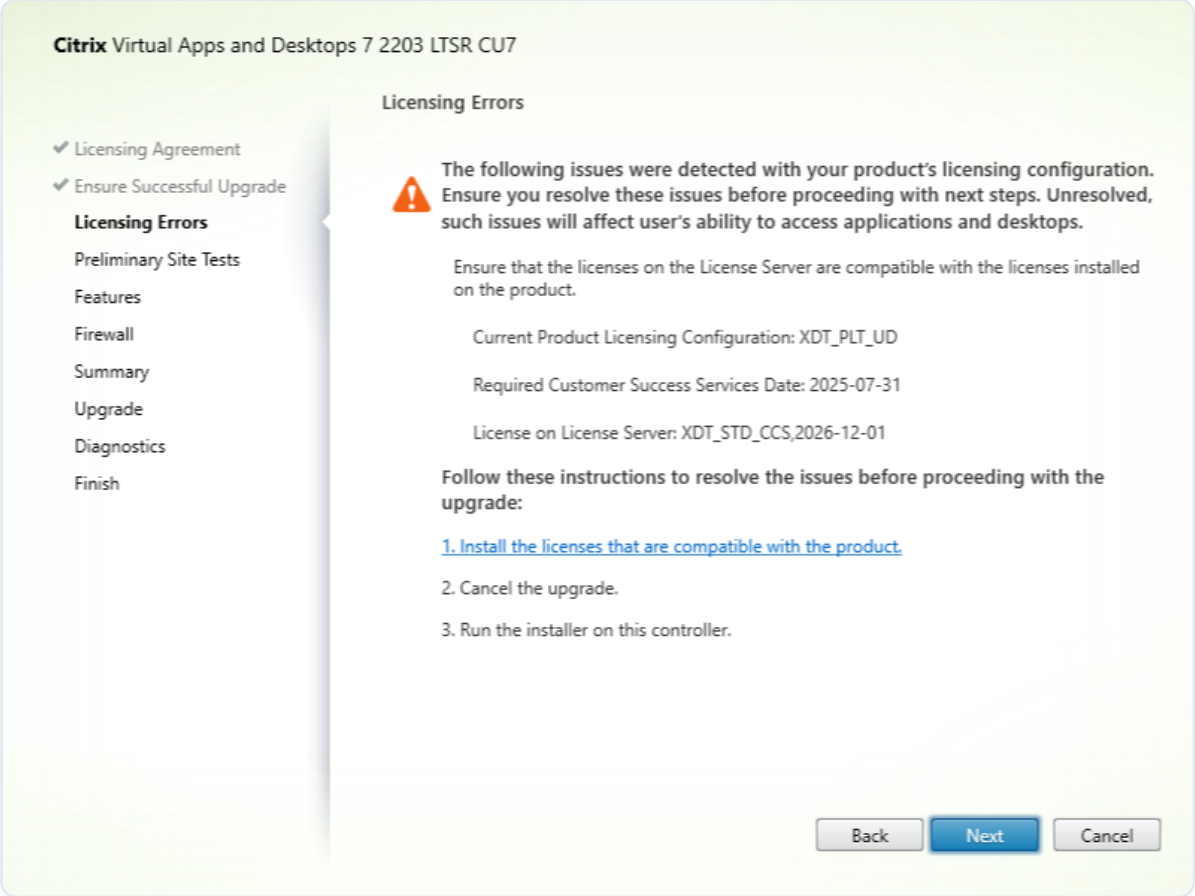
Considerações importantes para a atualização

Ao atualizar de qualquer versão anterior do Citrix Virtual Apps and Desktops para 2203 LTSR CU7 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 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 Servidor de Licenças 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, siga a mesma ordem para desinstalar:

1. Desinstalar 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`, limpe a entrada do registro e os arquivos restantes.

Para limpar as entradas do registro:

1. Procure a chave do registro `Citrix Licensing` e exclua essa entrada. Na maioria das vezes, você pode encontrar a entrada no seguinte local:

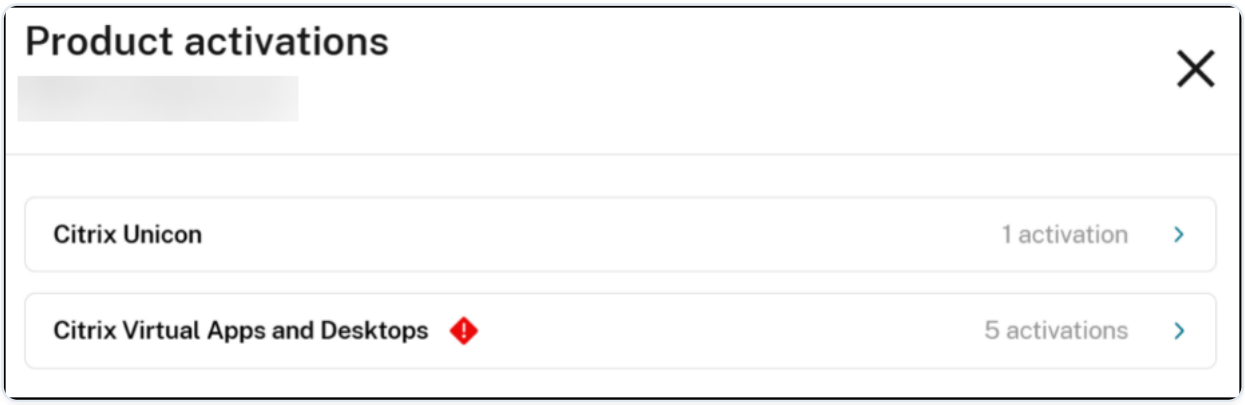
   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. Exclua a pasta apontada pela **Uninstall String** na chave do 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:

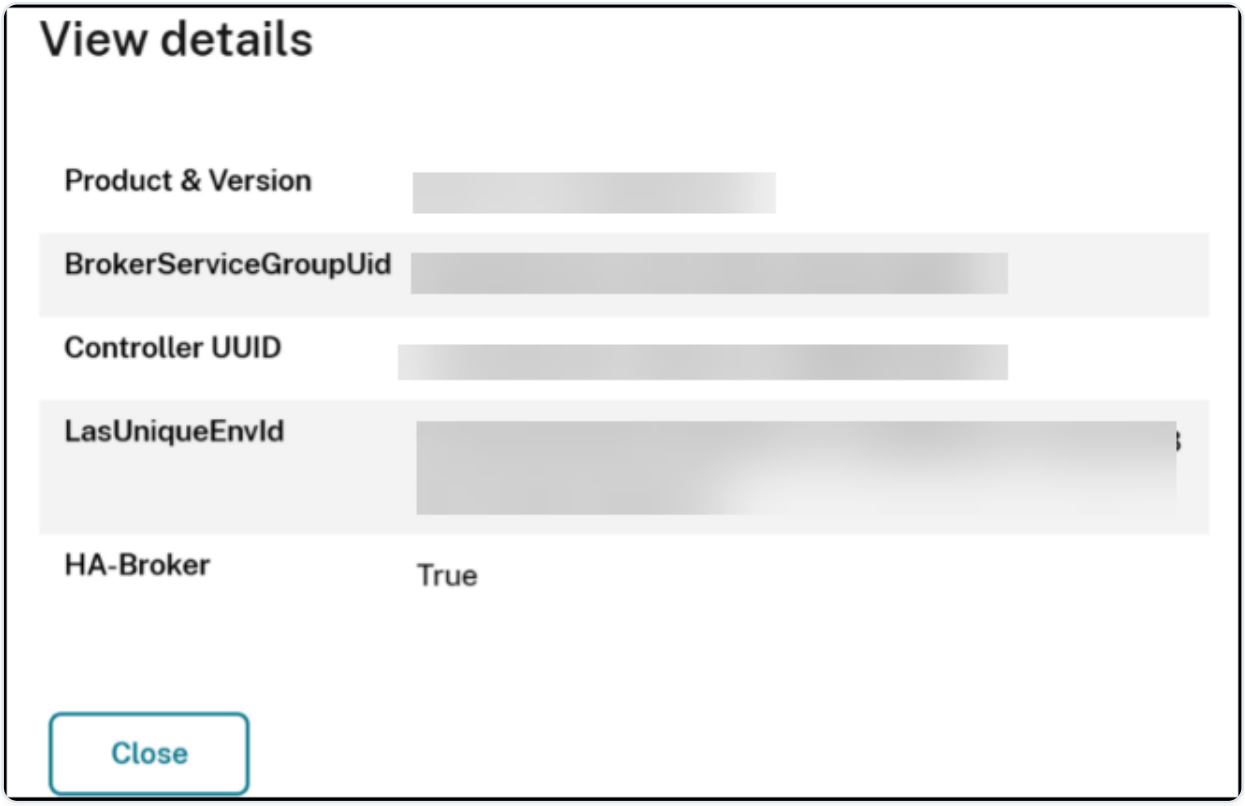
1. No Citrix Cloud, navegar para **Licenciamento > Implantações licenciadas > Servidores de licença**.
2. Clique no botão expandir **>** ao lado de Citrix Virtual Apps and Desktops para ver a lista de Delivery Controllers que foram ativados.



3. Clique em **Exibir detalhes** na 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 (Burn In Date) 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.
- **Controller UUID**: O UUID do Delivery Controller.
- **LasUniqueEnvId**: O ID exclusivo da instância fornecido 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 de Broker Citrix 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 de Broker Citrix contatou o servidor de licenças com sucesso.
1151	O Serviço de Broker Citrix 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 ao 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
	restante(s) antes que este controlador pare de fornecer sessões de desktop e aplicativos.
1155	O Serviço Citrix Broker agora parará de fornecer sessões de desktop e aplicativos. 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 do 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 Serviço Citrix Broker 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

ID DO EVENTO	DESCRIÇÃO
	relevantes do servidor de licenças para cumprir o limite de licenças.
1160	O serviço Citrix Broker 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 Citrix Broker 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 desnecessárias 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.

ID DO EVENTO	DESCRIÇÃO
1168	Erro ao ler as configurações de notificação do usuário de licenciamento. Verifique a conectividade do servidor de licenças.
1169	Este controlador entrou no modo de cache de licenças 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 aplicativos.
1170	O Serviço de Broker Citrix detectou com sucesso licenças adequadas no servidor de licenças. Este controlador não está mais no modo de cache de licenças pronto para uso.
1171	Nenhum servidor de licenças foi especificado. O Serviço de Broker Citrix 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 SDK do Citrix PowerShell.
1172	Erro ao verificar a adequação do servidor de licenças. O serviço de broker Citrix recebeu uma resposta inesperada ao verificar se uma máquina é adequada para uso como servidor de licenças. Verifique se a máquina pode ser contatada pelo 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 operando corretamente.
1173	Este site 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.

ID DO EVENTO	DESCRIÇÃO
1174	A edição do produto configurada para este site XenDesktop não oferece suporte a aplicativos; os recursos de aplicativo não estarão disponíveis.
1176	A edição do produto configurada não suporta máquinas multi-sessão. O registro foi rejeitado.
1177	A edição do produto configurada não suporta máquinas de sessão única. O registro foi rejeitado.
1178	A edição do produto configurada não suporta RemotePC. O registro foi rejeitado.
1179	A edição do produto configurada não suporta máquinas provisionadas em um sistema de nuvem. O registro foi rejeitado.
1180	A edição do produto configurada para este site XenDesktop não suporta 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 suporta aplicativos em máquinas multi-sessão (SO de servidor). O recurso do aplicativo teve o lançamento recusado.
1182	A edição do produto configurada para este site XenDesktop não suporta desktops em máquinas de sessão única (SO de estação de trabalho). O recurso da área de trabalho 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

ID DO EVENTO	DESCRIÇÃO
	servidor). O recurso de desktop teve seu lançamento recusado.
1196	Este controlador entrou em modo de burst 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 parará de fornecer sessões de desktop e aplicativo. Este controlador não está mais ou não conseguiu entrar em modo de burst 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 burst de licença causado pelo esgotamento de licenças.
1199	O Citrix Broker Service agora parará de fornecer sessões de desktop e aplicativo. Este controlador não está mais ou não conseguiu 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 está atualmente sem suporte. Verifique seu servidor de licenças para licenças expiradas e remova-as. Há um modo de cache de licença de 30 dias antes que os

ID DO EVENTO	DESCRIÇÃO
	usuários comecem a receber mensagens de aviso.
1206	O hash do certificado de licença é inválido. Seu hash do certificado de licença Citrix é inválido.
1300	O Citrix Broker Service agora parará de fornecer sessões de desktop e aplicativo. Há um problema com o relógio do sistema do servidor de licenças.
1301	Problemas com o relógio do sistema do servidor de licenças foram corrigidos. O Citrix Broker Service agora retomará a operação normal.
1302	Este controlador falhou novamente ao fazer check-in ou check-out de 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 Citrix Broker Service contatou o LAS com sucesso.
1305	O Citrix Broker Service 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?

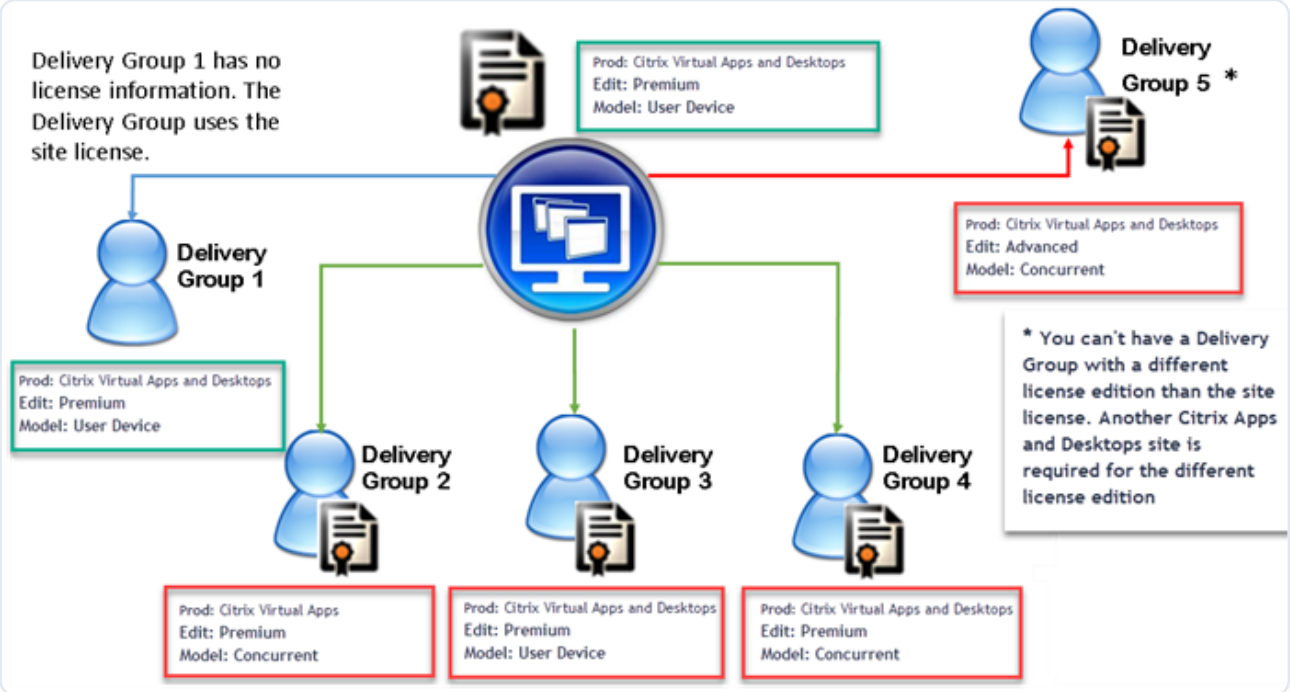
Para obter informações detalhadas sobre os comandos, consulte:

- 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 única combinação de ID do Produto (XDT ou MPS) e Modelo (UserDevice ou Concurrent). Os grupos de entrega devem usar a mesma Edição do Produto (PLT/Premium ou ENT/Advanced) 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 da licença ou do acionamento ou expiração do modo de burst da licença.
- Nenhuma notificação quando um grupo específico tem um problema.

Os grupos de entrega configurados para licenças de múltiplos tipos consomem APENAS esse tipo de licença e não retornam à configuração do site quando totalmente consumidos.

Embora os nomes das edições de licença Citrix Virtual Apps Standard e Citrix Virtual Desktops™ Standard indiquem que ambos são Standard, eles não são a mesma edição. O licenciamento de múltiplos tipos não está disponível com 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 múltiplos tipos. CCU e CCS significam licenças concorrentes e UD são licenças de usuário/dispositivo.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

SDK do PowerShell do Broker

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 desabilitada, a tentativa de definir uma propriedade falhará.
ProductCode	Uma string de texto de XDT (para Citrix Virtual Desktops) ou MPS (para Citrix Virtual Apps™) que especifica o ID do produto de licenciamento para o grupo. Se nenhum for especificado, o código do produto de todo o site será usado.	Se o alternador de recursos estiver desativado, 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 o agenciamento de grupos de desktops. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`.

Set-BrokerDesktopGroup

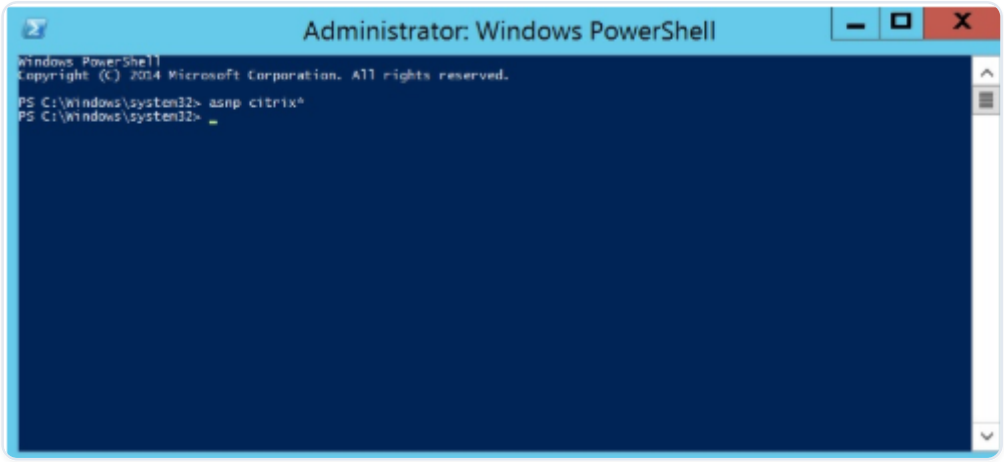
Desativa ou ativa um grupo de desktops de broker existente ou altera suas configurações. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`

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

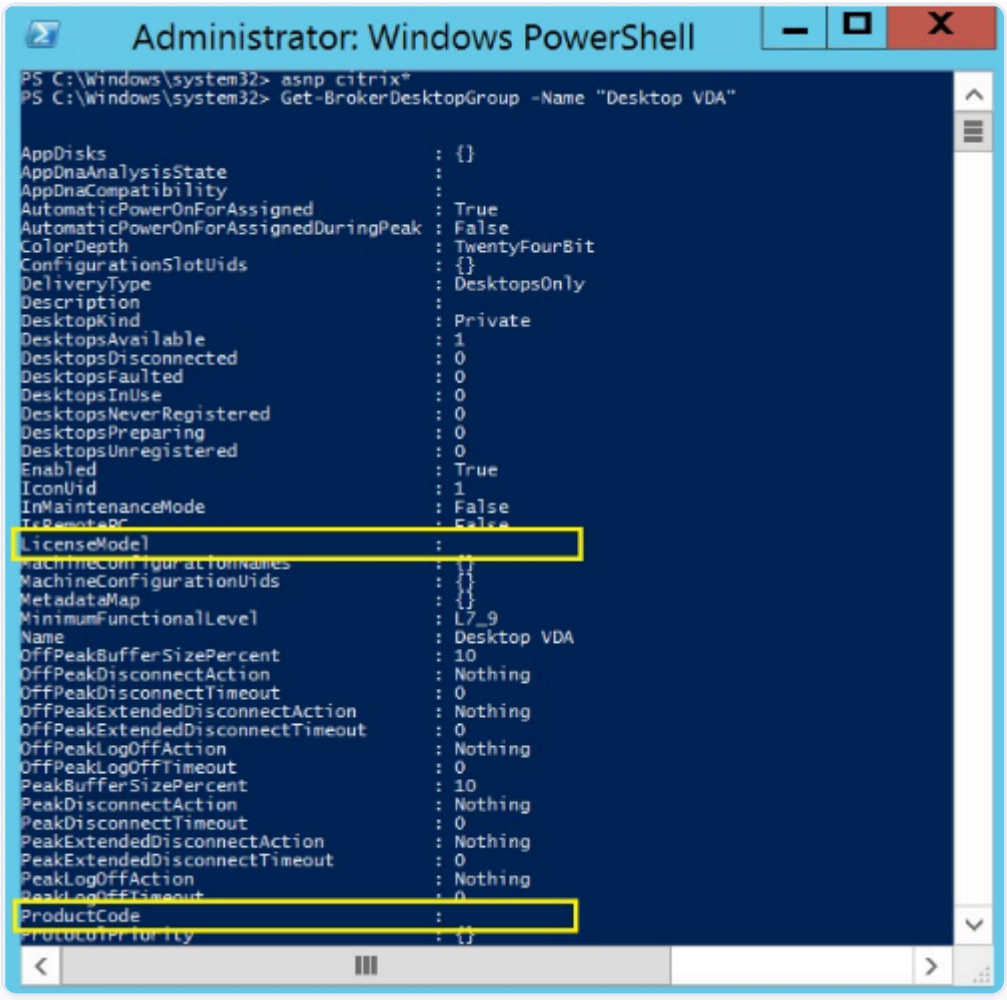
1. Abra o PowerShell com direitos administrativos e adicione o snap-in do Citrix.



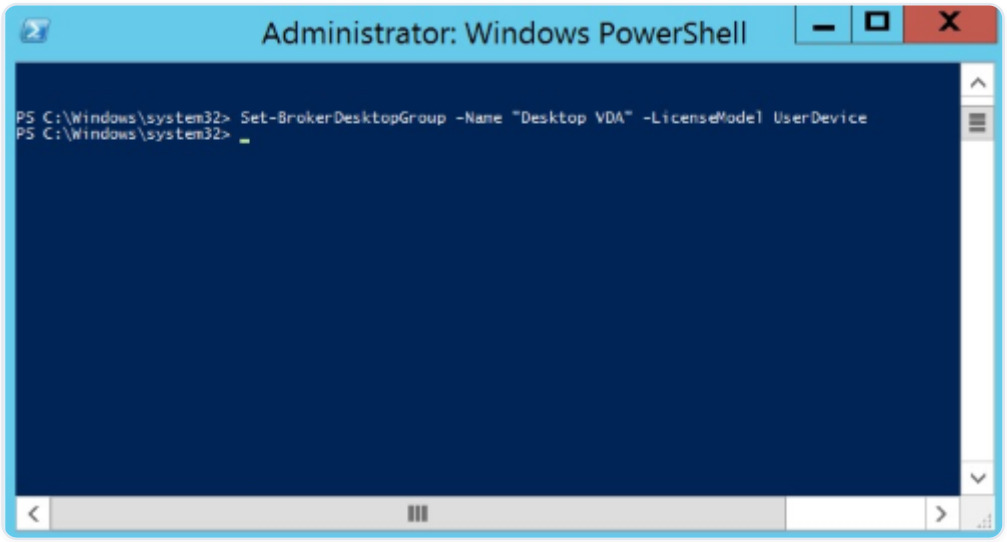
2. Execute o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para visualizar a configuração de licença atual. Encontre os parâmetros **LicenseModel** e **ProductCode**. Se você não configurou esses parâmetros antes, eles podem estar em branco.

> **Observação:**

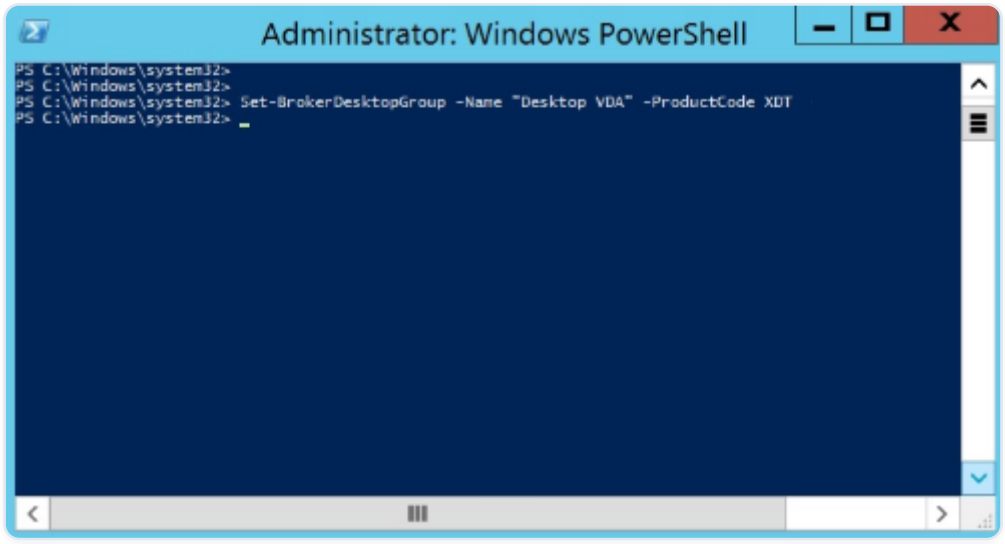
> Se um grupo de entrega não tiver informações de licença definidas, ele usará como padrão a **licença de site no nível do site**.



3. Altere o modelo de licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**.

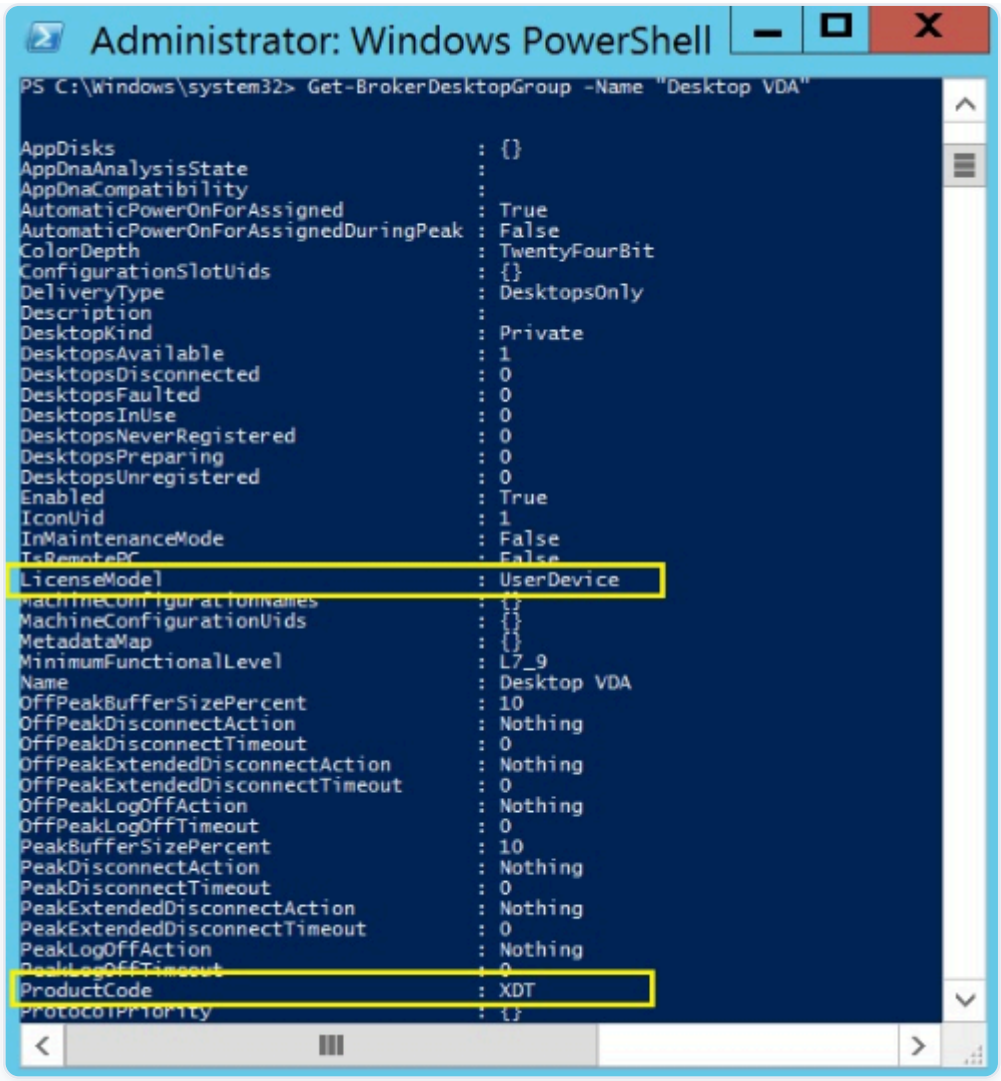


4. Altere o produto de licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**.



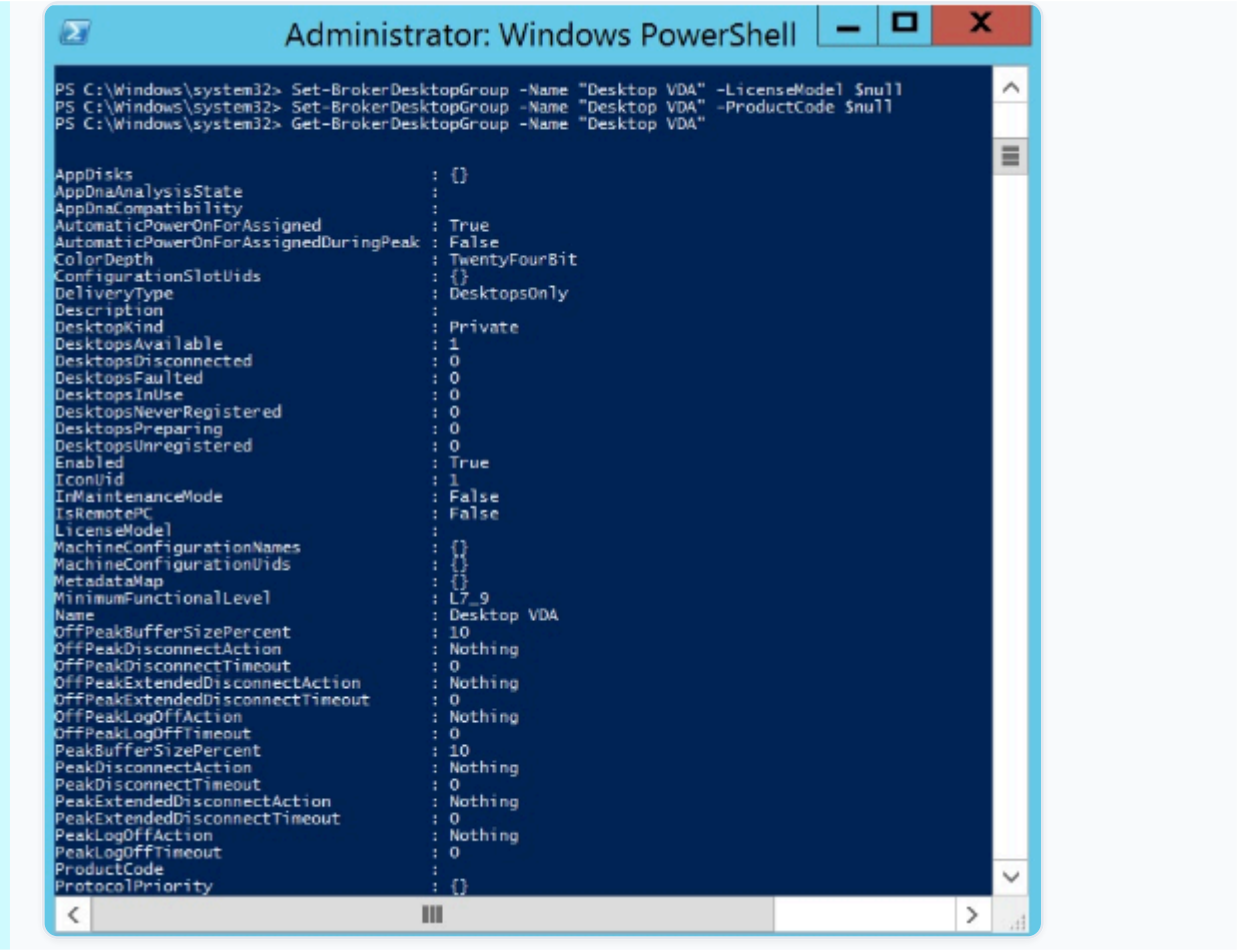
5. Insira o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para validar as alterações.

> **Observação:**
>
> Não é possível misturar e combinar edições no mesmo site. Por exemplo, licenças Premium e Advanced. Vários sites são necessários se você tiver licenças com edições diferentes.



6. Remova a configuração de licença executando os mesmos comandos **Set-BrokerDesktopGroup** conforme descrito nas etapas anteriores e defina o valor como **$null**.

> **Observação:**
>
> O Studio não exibe a configuração de licença para cada grupo de entrega. Use o PowerShell para visualizar a configuração atual.



Exemplo

Este exemplo de cmdlet PowerShell ilustra a configuração de licenciamento de múltiplos tipos para dois grupos de entrega existentes e cria e configura um terceiro grupo de entrega.

Para ver o produto de licença e o modelo de licença associados a um grupo de entrega, use o cmdlet 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. Definimos 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 Dispositivo de Usuário" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

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 Continuidade de negócios — sob demanda.
- Para obter mais informações sobre o Citrix License Server atual, consulte Licenciamento.

Licenciamento Citrix®

Como posso obter meu arquivo de licença?

Enviamos o código de acesso da licença por e-mail. Existem três maneiras de gerar arquivos de licença usando o código de acesso da licença:

- O **Gerenciar Licenças** na sua página MyAccount em `citrix.com`. Para obter mais informações, consulte Gerenciar licenças em citrix.com.
- Citrix Studio para alocar sua compra e o arquivo de licença é instalado automaticamente no seu Citrix License Server.
- Citrix Licensing Manager dentro do Citrix License Server para alocar sua compra e instalar seu arquivo de licença. Para obter mais informações, consulte Instalar licenças.

Como alocar licença na minha conta?

Consulte Alocar licenças.

Como adicionar licenças alocadas ao servidor de licenças?

Consulte Modificar licenças.

Quais portas TCP o licenciamento Citrix usa?

- O número da porta do Servidor de Licenças é 27000

- O número da porta do daemon do fornecedor é 7279
- A porta web do console de gerenciamento é 8082
- A porta do Serviço Web para Licenciamento é 8083

O que é o Servidor de Licenças Citrix?

O Servidor de Licenças Citrix 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 Servidor de Licenças Citrix?

Sim. Você pode virtualizar ou agrupar o Citrix License Server. Para obter mais informações, consulte Servidores de Licenças Agrupados.

Quais benefícios estão disponíveis para mim se eu virtualizar o Servidor de Licenças Citrix?

A virtualização do Servidor de Licenças Citrix 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 Servidor de Licenças Citrix?

Não.

O Servidor de Licenças Citrix 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 License Server no Citrix Cloud™ e fácil remoção do registro.
- Configurar contas de usuário e grupo.
- Usar o painel para exibir licenças instaladas, em uso, expiradas e disponíveis, e as datas dos 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 License Server usando um código de acesso de licença ou arquivo baixado.
- Ativar e desativar o modo de intermitência de licença.
- Configurar o Customer Experience Improvement Program (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 License Server - Licença de inicialização ausente, problemas de tempo, falhas do uploader.
- Modificar estas portas:
  - License Server (padrão 27000)
  - Vendor Daemon (padrão 7279)
  - Web Services for Licensing (padrão 8083)

Para obter mais informações, consulte Citrix Licensing Manager.

Onde está o Console de Administração de Licenças do Citrix?

O Console de Administração de Licenças não é mais suportado e foi removido do License Server versão 11.16.6. Recomendamos que você use o Citrix Licensing Manager.

Você pode usar o Studio para gerenciar e rastrear o licenciamento, desde que o License Server esteja no mesmo domínio do Studio ou em um domínio confiável.

Para obter mais informações, consulte Citrix Licensing Manager.

Qual é o período de atribuição de licença?

O período de atribuição de licença é o termo 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 adquiridas estão disponíveis para revisão e acesso a qualquer momento (24 horas por dia, 7 dias por semana) em sua caixa de ferramentas segura **Gerenciar Licenças** em sua página **Minha Conta** em `<https://www.citrix.com>`.

Como sei quantas licenças estão em uso a qualquer momento?

O Citrix Licensing Manager e o Studio fornecem detalhes sobre o uso 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 de 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 concorrente para clientes com usuários que precisam apenas de acesso ocasional aos seus desktops e aplicativos virtuais.

O licenciamento de usuário/dispositivo oferece aos usuários acesso aos seus desktops e aplicativos virtuais a partir de um número ilimitado de dispositivos. As licenças de dispositivo 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.

> **Concorrente:**

As licenças concorrentes 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 retornada ao pool.

Para obter mais informações sobre o licenciamento de usuário/dispositivo, consulte Licença de usuário/dispositivo e para licenças concorrentes, consulte Licença concorrente.

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 localmente 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 concorrência para o Citrix Virtual Apps and Desktops?

O modelo concorrente 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 retornada ao pool para reemissão. Para obter mais informações, consulte Licença concorrente.

Posso implantar várias edições de licenças do Citrix Virtual Apps and Desktops em um servidor de licenças 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 concorrente. Um único site do Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode suportar apenas uma edição. Para obter mais informações, consulte Licenciamento de vários tipos.

As versões mínimas que suportam licenciamento de vários tipos são XenApp e XenDesktop 7.15 Long Term Service Release (LTSR) e Citrix Virtual Apps and Desktops 7 1808.

Posso selecionar o Citrix Virtual Apps concorrente como modelo de produto se tiver licenças de usuário/dispositivo do Citrix Virtual Apps and Desktops ou licenças concorrentes do Citrix Virtual Apps and Desktops instaladas no 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 para o Citrix Virtual Apps 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 para este produto, mesmo que planeje usar apenas a funcionalidade de aplicativos virtuais. Selecione o Citrix Virtual Apps como um modelo de produto somente se você tiver licenças autônomas concorrentes deste produto instaladas no License Server.

Quais componentes do produto estão incluídos em cada edição do Citrix Virtual Apps e do Citrix Virtual Apps and Desktops?

Para uma matriz completa de recursos por edição, consulte Recursos do Citrix Virtual Apps and Desktops.

Como licencio ambientes Citrix Virtual Desktops™ em conformidade com o EULA do Citrix Virtual Apps and Desktops?

Para implantar o Citrix Virtual Apps and Desktops sob o modelo de licença de usuário/dispositivo ou concorrente em conformidade com o EULA do Citrix Virtual Apps and Desktops, aplique os arquivos de licença ao seu 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 obter mais informações, consulte o Centro de Conformidade de Licenças de Produto.

Como licencio ambientes Citrix Virtual Apps em conformidade com o EULA do Citrix Virtual Apps?

Para implantar o Citrix Virtual Apps sob o modelo de licença concorrente em conformidade com o EULA do Citrix Virtual Apps, aplique os arquivos de licença ao seu License Server. O License Server então controla e monitora a conformidade da licença.

Existe um requisito de licenciamento para as opções de serviço do Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) ou Current Release (CR)?

As Opções de Serviço do Citrix Virtual Apps and Desktops, como a Versão de Serviço de Longo Prazo, são um benefício do programa Customer Success Services. Você deve ter o Customer Success Services ativo para se qualificar para os benefícios do LTSR. Para obter mais

informações, consulte [Citrix Virtual Apps, Citrix Virtual Apps and Desktops e Citrix Hypervisor Servicing Options.

Como funcionam as horas agrupadas do serviço Remote Browser Isolation (RBI)?

Ao adquirir um mínimo de 25 usuários do serviço, você recebe 5000 horas de direitos para usar o serviço, agrupadas entre todos os usuários. Compras subsequentes de direitos de usuário não aumentam o direito a horas agrupadas. Para aumentar o direito a horas de serviço, compre pacotes de complementos.

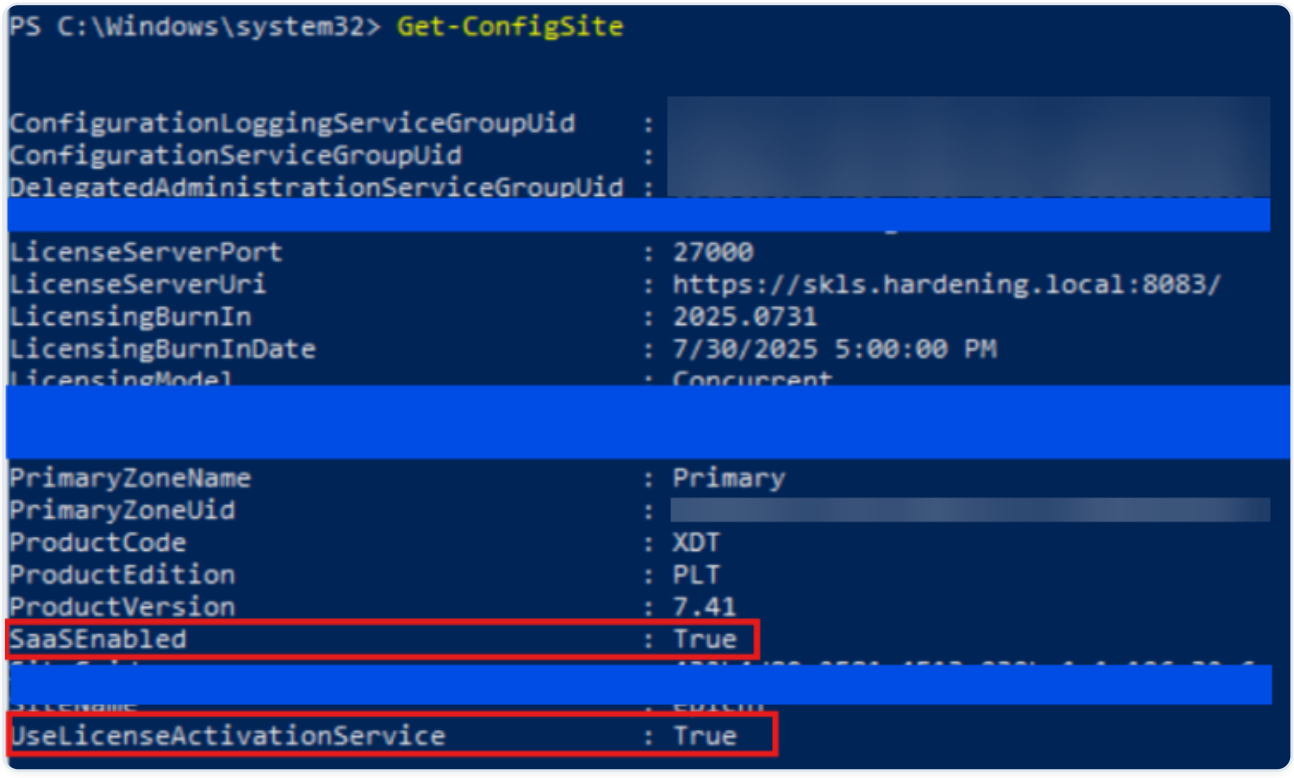
Posso usar o Remote PC Access com licenças CCU?

Sim.

Para obter informações sobre o Remote PC Access, consulte Remote PC Access.

Como posso verificar o estado LAS de um site?

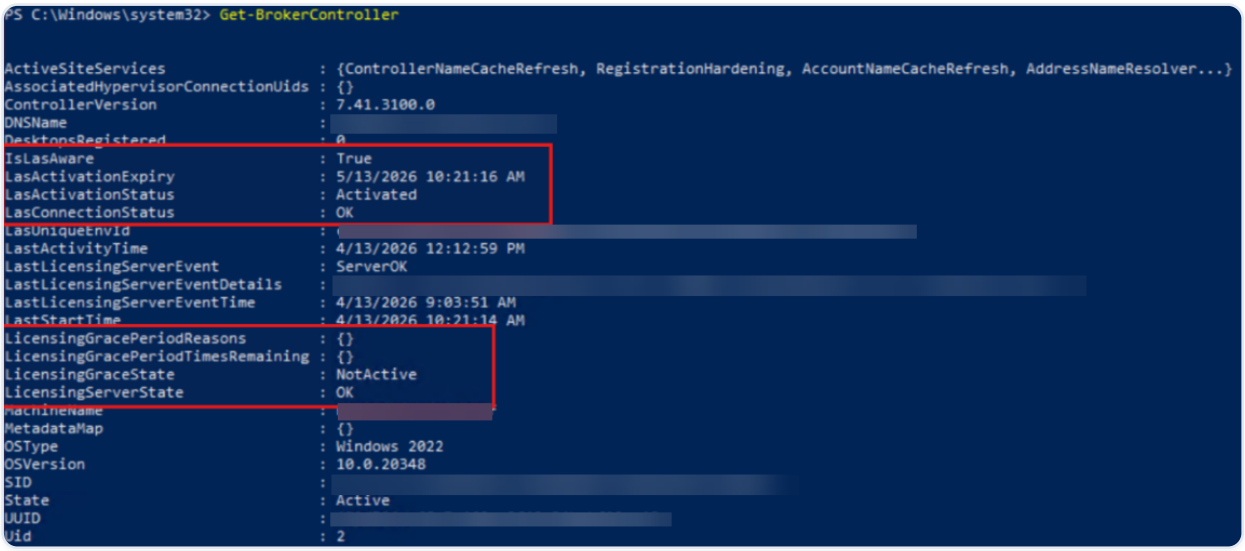
Execute `Get-configsite` para verificar o estado de ativação do LAS e o status do bit SaaS.



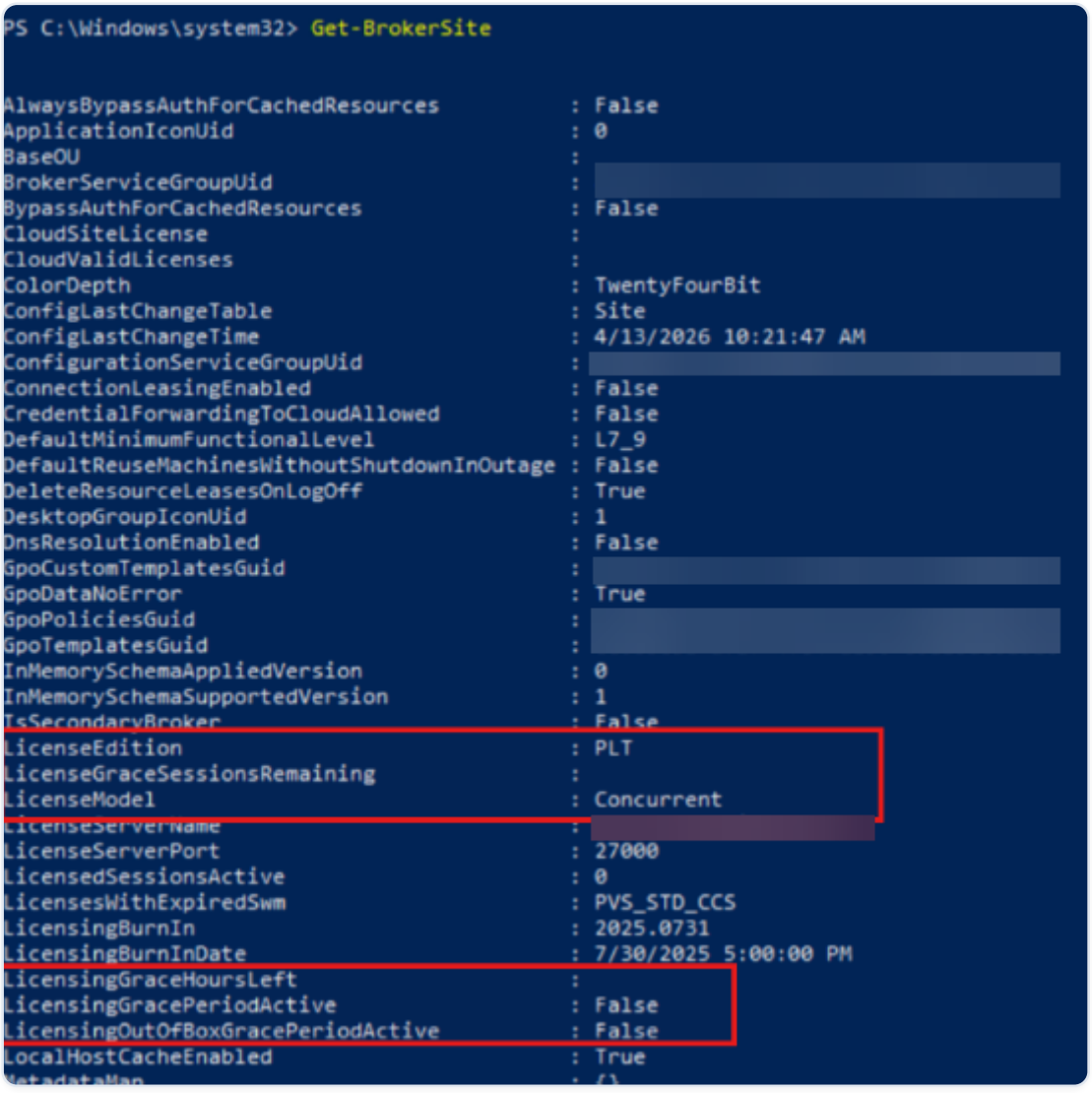
Como posso verificar se um site está no modo de cache de licença?

Execute `Get-Brokercontroller` e `Get-brokersite` para obter detalhes sobre o modo de cache 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 Servidor de Licenças 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 Servidor de Licenças ou o serviço de nuvem atribui a licença. Você não pode atribuir essas licenças manualmente. A licença é atribuída ao usuário, não ao dispositivo compartilhado. Uma vez atribuída, a licença não pode ser atribuída a outro usuário antes de 90 dias de inatividade. Para 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 simultâneas do Citrix Virtual Desktops Standard Edition para o modelo de usuário/dispositivo?

Você não pode converter licenças simultâneas 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 simultâneas do Citrix Virtual Desktops Standard Edition.

Se você tiver licenças simultâneas 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 SIMULTÂNEO 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	Não é possível converter modelos de licença, mas você pode fazer upgrade para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.	Não é possível converter modelos de licença, mas você 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 de usuário/ dispositivo?

Baseamos o licenciamento simultâneo em conexões de dispositivos simultâneas. Uma licença simultânea é usada 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. Não é possível 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 de 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.

No modelo de usuário/dispositivo, qual é o número máximo de usuários que podem acessar um dispositivo licenciado?

Cada dispositivo licenciado pode atender um número ilimitado de usuários dentro de uma organização.

No 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 comprar 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 comprar 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 autorizada?

Para liberar a atribuição de um usuário/dispositivo autorizado, use o utilitário `udadmin` de acordo com os termos do EULA. O License Server então atribui a licença ao próximo usuário/dispositivo apropriado. Para obter mais informações, consulte Exibir ou liberar licenças para usuários ou dispositivos.

O que acontece se eu exceder minha contagem de licenças de usuário/dispositivo compradas?

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. Compre 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 estouro de licenças (license burst mode) permite conexões ilimitadas a um produto. O modo de estouro de licenças oferece 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 estouro de licenças.

O Director exibe os estados do modo de cache de licenças. Para obter mais informações, consulte Painéis no Director Dashboard.

Qual é o número máximo de aplicativos virtuais que um usuário licenciado pode consumir a qualquer momento?

Cada usuário licenciado pode se conectar a um número ilimitado de aplicativos virtuais.

O que acontece se um usuário licenciado sair da minha organização?

Quando um usuário licenciado existente sai da sua organização, você pode liberar a licença do usuário que está saindo sem notificar a Citrix. Use o utilitário `udadmin` para liberar a licença. Se você não liberar a licença, o License Server 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 na minha organização?

Se você substituir um dispositivo licenciado existente, 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 um dispositivo licenciado estiver fora de serviço por um período prolongado?

Quando um dispositivo licenciado existente está 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 License Server 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 ocorre automaticamente. O License Server atribui licenças a usuários ou dispositivos com base nos padrões de uso. Se os padrões de uso mudarem, o License Server pode alternar a atribuição com base no novo uso. O License Server sempre atribui licenças da maneira mais econômica para o cliente. Além disso, o License Server 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 License Server?

Sim. Você pode continuar a usar o mesmo License Server 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 de 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 do Citrix Virtual Apps and Desktops Advanced e Premium 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 adquiridas?

Se todas as licenças estiverem em uso, o modo de estouro de licença permite conexões ilimitadas a um produto. O modo de estouro 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 mais informações, consulte Modo de estouro de licença.

O Director exibe os estados do modo de cache de licença. Para mais informações, consulte Painéis no Painel do Director.

Licenças de excedente

Como obtenho licenças de excedente?

Produtos (excluindo Citrix Cloud) que suportam modelos de licença de usuário/dispositivo, usuário ou dispositivo incluem um recurso de excedente de licença que permite usar um número limitado de licenças extras para evitar a negação de acesso. Oferecemos qualquer recurso de excedente como uma conveniência, não como um direito de licença. Licenças simultâneas e de servidor não contêm excedente. Quaisquer licenças de excedente usadas devem ser adquiridas dentro de 30 dias do primeiro uso, mas o uso não é limitado a 30 dias. A Citrix reserva-se o direito de remover qualquer recurso de excedente em novos lançamentos de produtos. Para mais informações, consulte Excedente de licença.

Como posso identificar um excedente de licença?

Você pode visualizar informações de uso, incluindo o número de licenças em excedente no Citrix Licensing Manager. O Studio também contém informações de uso de excedente.

O que acontece quando uma licença de excedente 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 excedente oferece o mesmo acesso e funcionalidade que as suas outras licenças.

Posso receber um alerta quando minhas licenças de excedente forem consumidas?

Atualmente, não há alertas específicos fornecidos quando licenças de overdraft são consumidas.

Por quanto tempo uma licença de overdraft pode ser consumida?

Adquira quaisquer licenças de overdraft usadas dentro de 30 dias do primeiro uso.

Outras informações de licenciamento específicas do produto

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor
- Citrix Licensing

Aplicativos

Introdução

Se sua implantação usa apenas grupos de entrega (e não grupos de aplicativos), você adiciona aplicativos aos grupos de entrega. Se você também tiver grupos de aplicativos, geralmente adiciona aplicativos aos grupos de aplicativos. Esta orientação facilita a administração. Um aplicativo deve sempre pertencer a pelo menos um grupo de entrega ou grupo de aplicativos.

No assistente Adicionar Aplicativos, você pode selecionar um ou mais grupos de entrega, ou um ou mais grupos de aplicativos, mas não ambos. Embora você possa alterar posteriormente a associação de grupo de um aplicativo (por exemplo, mover um aplicativo de um grupo de aplicativos para um grupo de entrega), a melhor prática desencoraja adicionar essa complexidade. Mantenha seus aplicativos em um único tipo de grupo.

Quando você associa um aplicativo a mais de um grupo, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses

casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo está associado.

Se você publicar dois aplicativos com o mesmo nome (talvez de grupos diferentes) para os mesmos usuários, altere a propriedade `Application name (for user)` no Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace™.

Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Você também pode alterar a pasta do aplicativo onde o aplicativo é colocado, seja ao adicionar o aplicativo ou posteriormente.

Para obter detalhes, consulte:

- Criar grupos de entrega
- Criar grupos de aplicativos
- Tags

Adicionar aplicativos

Você pode adicionar aplicativos ao criar um grupo de entrega ou um grupo de aplicativos. Esses procedimentos são detalhados em Criar grupos de entrega e Criar grupos de aplicativos. O procedimento a seguir descreve como adicionar aplicativos depois de criar um grupo.

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega do Remote PC Access.
- Você não pode usar o assistente Adicionar Aplicativo para remover aplicativos de grupos de entrega ou grupos de aplicativos. Essa é uma operação separada.

Para adicionar um ou mais aplicativos:

1. Selecione **Aplicativos** no painel de navegação do Studio e, em seguida, selecione **Adicionar Aplicativos** no painel Ações.
2. O assistente Adicionar Aplicativos é iniciado com uma página de **Introdução**, que você pode remover de futuros lançamentos deste assistente.
3. O assistente o guia 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 de navegação do Studio, selecione um grupo de entrega no painel central e, em seguida, selecione **Adicionar Aplicativos** no painel Ações. O assistente não exibe a página **Grupos**.
- **Para adicionar aplicativos a apenas um grupo de aplicativos:** Na etapa 1, selecione **Aplicativos** no painel de navegação do Studio, selecione um grupo de aplicativos no painel central e, em seguida, selecione a entrada **Adicionar Aplicativos** sob o nome do grupo de aplicativos no painel Ações. O assistente não exibe a página **Grupos**.

Página Grupos

Esta página lista todos os grupos de entrega no site. Se você também criou grupos de aplicativos, a página lista os grupos de aplicativos e os grupos de entrega. Você pode escolher entre um dos grupos, mas não de ambos. Em outras palavras, você não pode adicionar aplicativos a um grupo de aplicativos e a um grupo de entrega ao mesmo tempo. Geralmente, se você estiver usando grupos de aplicativos, adicione aplicativos a grupos de aplicativos, em vez de grupos de entrega.

Ao adicionar um aplicativo, marque a caixa de seleção ao lado de pelo menos um grupo de entrega (ou grupo de aplicativos, se disponível). Todo aplicativo deve estar sempre associado a pelo menos um grupo.

Página Aplicativos

Clique em **Adicionar** para exibir as fontes de aplicativos.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta fonte não pode ser selecionada se você (1) selecionou grupos de aplicativos sem grupos de entrega associados, (2) selecionou grupos de aplicativos com grupos de entrega associados que não contêm máquinas, ou (3) selecionou um grupo de entrega que não contém máquinas.
- **Definido manualmente:** Aplicativos localizados no site ou em outro lugar na sua rede. Ao selecionar esta fonte, uma nova página é iniciada. Insira o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Após inserir essas informações, clique em **OK**.

- **Existente:** Aplicativos adicionados anteriormente ao site. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta origem não pode ser selecionada se o site não tiver aplicativos.

- **App-V:** Aplicativos em pacotes App-V. Ao selecionar esta fonte, uma nova página é iniciada onde você seleciona o servidor App-V ou a 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 App-V.

  Esta origem não pode ser selecionada se o App-V não estiver configurado para o site.

- **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. Selecione as caixas de seleção dos grupos de aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta origem não pode ser selecionada se (1) não houver grupos de aplicativos, ou (2) se os grupos de entrega selecionados não suportarem grupos de aplicativos (por exemplo, grupos de entrega com máquinas atribuídas estaticamente).

Conforme observado na tabela, algumas origens na lista **Adicionar** não podem ser selecionadas se não houver uma origem válida desse tipo. As origens incompatíveis (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos) não são incluídas na lista. Os aplicativos que já foram adicionados aos grupos que você escolheu não podem ser selecionados.

Você pode alterar as propriedades (configurações) de um aplicativo a partir desta página, ou mais tarde.

Por padrão, os aplicativos adicionados são colocados na pasta de aplicativos chamada `Applications`. Você pode alterar o aplicativo a partir desta página, ou mais tarde. 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 existir 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 no painel Ações.

Se um aplicativo estiver associado a mais de um grupo de entrega ou de aplicativos, a prioridade do grupo pode ser usada para especificar a ordem em que vários grupos são verificados para encontrar aplicativos. Por padrão, todos os grupos têm prioridade 0 (a mais alta). Grupos com a mesma prioridade são balanceados por carga.

Um aplicativo pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos. Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam apenas desktops, se (1) o grupo de entrega contiver máquinas compartilhadas e tiver sido criado com uma versão do XenDesktop 7.x anterior a 7.9, e (2) você tiver permissão `Edit delivery group`. O tipo de grupo de entrega é automaticamente convertido para `desktops and applications` quando a caixa de diálogo de propriedades é confirmada.

1. Selecione **Aplicativos** no painel de navegação do Studio e, em seguida, selecione o aplicativo no painel central.
2. Selecione **Propriedades** no painel 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 aplicação não estar mais associada a nenhum grupo, você será alertado de que a aplicação será excluída.

- Para alterar a prioridade de um grupo, selecione o grupo e clique em **Editar Prioridade**. Selecione um valor de prioridade e clique em **OK**.

4. Quando terminar, clique em **Aplicar** para aplicar as alterações e deixar a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Duplicar, habilitar ou desabilitar, renomear ou excluir um aplicativo

As seguintes ações estão disponíveis:

- **Duplicar:** Você pode querer duplicar um aplicativo para criar uma versão diferente com parâmetros ou propriedades distintas. Ao duplicar um aplicativo, ele é automaticamente renomeado com um sufixo exclusivo e colocado ao lado do original. Você também pode querer duplicar um aplicativo e depois adicioná-lo a um grupo diferente. (Após a duplicação, a maneira mais fácil de mover um aplicativo é arrastando-o.)
- **Habilitar ou desabilitar:** Habilitar e desabilitar um aplicativo é uma ação diferente de habilitar e desabilitar um grupo de entrega ou grupo de aplicativos.
- **Renomear:** Você pode renomear apenas um aplicativo por vez. Se você tentar renomear um aplicativo e já existir um com o mesmo nome na mesma pasta ou grupo, será solicitado que você especifique um nome diferente.
- **Excluir:** A exclusão de um aplicativo o remove dos grupos de entrega e grupos de aplicativos aos quais estava associado, mas não da origem que foi usada para adicionar o aplicativo originalmente. Excluir um aplicativo é uma ação diferente de removê-lo de um grupo de entrega ou grupo de aplicativos.

Para duplicar, habilitar, desabilitar, renomear ou excluir um aplicativo:

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione um ou mais aplicativos no painel central e, em seguida, selecione a tarefa apropriada no painel Ações.
3. Confirme a ação, quando solicitado.

Remover aplicativos de um grupo de entrega

Um aplicativo deve estar associado (pertencer) a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de entrega que removeria a associação desse aplicativo com qualquer grupo de entrega ou grupo de aplicativos, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontece, se você quiser entregar esse aplicativo, você deve adicioná-lo novamente de uma fonte válida.

1. Selecione **Grupos de Entrega** no painel de navegação do Studio.
2. Selecione um grupo de entrega. No painel central inferior, na guia **Aplicativos**, selecione o aplicativo que deseja remover.
3. Selecione **Remover Aplicativo** no painel 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, o que resultaria na não pertença desse aplicativo a nenhum grupo, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontece, se você quiser entregar esse aplicativo, você deve adicioná-lo novamente de uma fonte válida.

1. Selecione **Aplicativos** no painel de navegação do Studio.
2. Selecione o grupo de aplicativos no painel central e, em seguida, selecione um ou mais aplicativos.
3. Selecione **Remover do Grupo de Aplicativos** no painel 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 de navegação do Studio.
2. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** no painel 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

PROPRIEDADE	PÁGINA
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
Caminho para o executável; consulte Passar parâmetros para aplicativos publicados	Localização
Atalho na área de trabalho do usuário: ativar ou desativar	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 os limites de aplicativo para ajudar a gerenciar o uso do aplicativo. Por exemplo, você pode usar os 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.

Esse recurso limita o número de inicializações de aplicativos que são intermediadas pelo Controller (por exemplo, do Citrix Workspace app e do StoreFront), e não o número de aplicativos em execução que podem ser iniciados por outros métodos. Isso significa que os limites de aplicativos auxiliam os administradores no gerenciamento do uso simultâneo, mas não fornecem imposição em todos os cenários. Por exemplo, os limites de aplicativos não podem ser aplicados quando o Controller está em 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 aplicativos:

- **Limite de número 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 um aplicativo por usuário:** Em outro grupo de entrega, você habilita a opção de uma instância por usuário para o aplicativo `Beta`. O usuário Tony inicia o aplicativo `Beta` com sucesso. Mais tarde no dia, enquanto esse aplicativo ainda está em execução na sessão

de Tony, ele tenta iniciar outra instância de `Beta`. Uma mensagem de erro é gerada e `Beta` não é iniciado porque excederia o limite de uma instância por usuário.

- **Número máximo de instâncias simultâneas e limites de uma instância por usuário:** Em outro grupo de entrega, você configura um número máximo de instâncias simultâneas de 10 e habilita a opção de uma instância por usuário para o aplicativo `Delta`. Mais tarde, quando 10 usuários nesse grupo de entrega tiverem cada um uma instância de `Delta` em execução, qualquer outro usuário nesse grupo de entrega que tentar iniciar `Delta` receberá uma mensagem de erro. `Delta` não é iniciado. Se qualquer um dos 10 usuários atuais de `Delta` tentar iniciar uma segunda instância desse aplicativo, eles receberão uma mensagem de erro e a segunda instância não será iniciada.
- **Número máximo de instâncias simultâneas por máquina e 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 do site):

  - Use a funcionalidade de marcação para essas máquinas.
  - Configure o número máximo de instâncias por limite de máquina para esse aplicativo.

Se os aplicativos forem iniciados por métodos diferentes da intermediação do Controller (por exemplo, enquanto um Controller estiver em modo de interrupção) e os limites configurados forem excedidos, os usuários não poderão iniciar mais instâncias até que fechem instâncias suficientes para não exceder mais os limites. As instâncias que excederam o limite não são encerradas à força. Elas terão permissão para continuar até que seus usuários as fechem.

Se você desabilitar o roaming de sessão, desabilite o limite de uma instância por usuário para o aplicativo. Se você habilitar o limite de uma instância por usuário para o aplicativo, não configure

nenhum dos dois valores que permitem novas sessões em novos dispositivos. Para obter informações sobre roaming, consulte Sessões.

Para configurar o limite máximo de instâncias por grupo de entrega e o limite de uma instância por usuário:

1. Selecione **Aplicativos** no painel de navegação do Studio e, em seguida, selecione um aplicativo.
2. Selecione **Editar Propriedades do Aplicativo** no painel Ações.
3. Na página **Entrega**, escolha uma das seguintes opções.
    - **Permitir uso ilimitado do aplicativo**. Não há limite para o número de instâncias em execução ao mesmo tempo. Este é o padrão.
    - **Definir limites para o aplicativo**. Existem dois tipos de limite; especifique um ou ambos.
        - Especifique o número máximo de instâncias que podem ser executadas simultaneamente
        - Limitar a uma instância do aplicativo por usuário
4. Clique em **OK** para aplicar a alteração e fechar a caixa de diálogo, ou em **Aplicar** para aplicar a alteração e deixar a caixa de diálogo aberta.

Para configurar o limite máximo de instâncias por máquina (somente PowerShell):

- No PowerShell (usando o SDK do PowerShell Remoto para implantações do Citrix Cloud™ ou o SDK do PowerShell para implantações locais), insira o cmdlet `BrokerApplication` 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 **Localização** das propriedades de um aplicativo para inserir a linha de comando e passar parâmetros para aplicativos publicados.

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos `"%*"` (símbolos de porcentagem e asterisco entre aspas duplas) são anexados ao final da linha de comando do aplicativo. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos de usuário.

Se um aplicativo publicado não iniciar conforme o esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos 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 para o aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Para fazer isso, adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos `%*`. Certifique-se de incluir um espaço entre as aspas de fechamento do caminho e as aspas de abertura dos símbolos `%*`.

Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **Observação:**
>
> O número máximo de caracteres, incluindo argumentos, na linha de comando para iniciar aplicativos publicados é 203.

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 Applications, mas pode mover todos os aplicativos que ela contém para outras pastas que você criar.
- Um nome de pasta pode conter de 1 a 64 caracteres. Espaços são permitidos.
- As pastas podem ser aninhadas em até cinco níveis.
- As pastas não precisam conter aplicativos. Pastas vazias são permitidas.
- As pastas são listadas em ordem alfabética no Studio, a menos que você as mova ou especifique um local diferente ao criá-las.

- Você pode ter mais de uma pasta com o mesmo nome, desde que cada uma tenha uma pasta pai diferente. Da mesma forma, você pode ter mais de um aplicativo com o mesmo nome, desde que cada um esteja em uma pasta diferente.
- Você deve ter permissão `View Applications` para ver os aplicativos nas pastas, e deve ter permissão `Edit Application Properties` para todos os aplicativos na pasta para remover, renomear ou excluir uma pasta que contém aplicativos.
- A maioria dos procedimentos a seguir solicita ações usando o painel Ações no Studio. Alternativamente, você pode usar menus de clique com o botão direito ou arrastar o item. Por exemplo, se você criar ou mover uma pasta para um local que não pretendia, pode arrastá-la/soltá-la para o local correto.

Para gerenciar pastas de aplicativos, selecione **Aplicativos** no painel de navegação do Studio. Use a lista a seguir para orientação.

- **Para visualizar todas as pastas (excluindo pastas aninhadas):** Clique em **Mostrar tudo** acima da lista de pastas.
- **Para criar uma pasta no nível mais alto (não aninhada):** Selecione a pasta **Aplicativos**. Para colocar a nova pasta sob uma pasta existente que não seja **Aplicativos**, selecione essa pasta. Em seguida, selecione **Criar Pasta** no painel Ações. Digite um nome.
- **Para mover uma pasta:** Selecione a pasta e, em seguida, selecione **Mover Pasta** no painel 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** no painel Ações. Digite um nome.
- **Para excluir uma pasta:** Selecione a pasta e, em seguida, selecione **Excluir Pasta** no painel 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** no painel Ações. Selecione a pasta.

Você também pode colocar os aplicativos que está adicionando em uma pasta na página **Aplicativo** ao criar um grupo de entrega ou um grupo de aplicativos. Por padrão, os aplicativos adicionados vão para a pasta **Aplicativos**. Clique em **Alterar** para selecionar ou criar uma pasta.

Controlar o lançamento local de aplicativos em desktops publicados

Quando os usuários iniciam um aplicativo publicado de dentro de um desktop publicado, você pode controlar se o aplicativo é iniciado nessa sessão de desktop ou como um aplicativo publicado. O aplicativo Citrix Workspace procura o caminho de instalação do aplicativo no registro do Windows no VDA e, se presente, inicia a instância local do aplicativo. Caso contrário, uma instância hospedada do aplicativo é iniciada. Se você iniciar um aplicativo que não está instalado no VDA, o aplicativo hospedado será iniciado. Para obter mais informações, consulte início vPrefer.

No PowerShell (usando o SDK do PowerShell Remoto em implantações do Citrix Cloud ou o SDK do PowerShell em implantações locais), você pode alterar essa ação.

No cmdlet `New-Broker` Application ou `Set-BrokerApplication`, use a opção `LocalLaunchDisabled`. Por exemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Por padrão, o valor desta opção é falso (`-LocalLaunchDisabled $false`). Ao iniciar um aplicativo publicado de dentro de um desktop publicado, o aplicativo é iniciado nessa sessão de desktop.

Se você definir o valor da opção como verdadeiro (`-LocalLaunchDisabled $true`), o aplicativo publicado será iniciado. Isso cria uma sessão separada e adicional do desktop publicado (usando o aplicativo Citrix Workspace para Windows) para o aplicativo publicado.

Requisitos e limites:

- O valor `ApplicationType` do aplicativo deve ser `HostedOnDesktop`.
- Esta opção está disponível apenas por meio do SDK do PowerShell apropriado. Atualmente, ela não está disponível na interface gráfica do Studio.
- Esta opção requer o mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 e Delivery Controller 7.17.

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: Os 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 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.

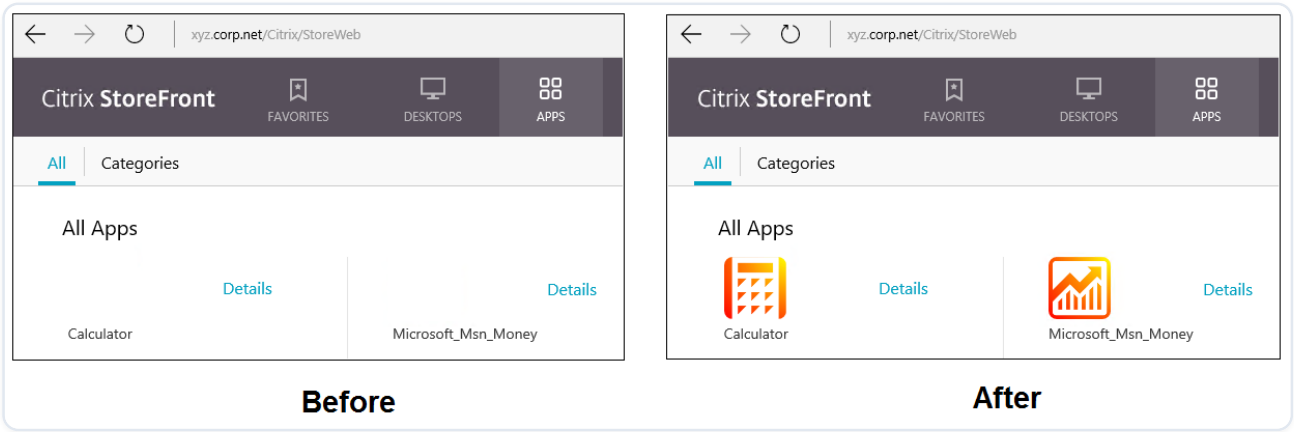
Durante o sideload, o aplicativo UWP é instalado na máquina e fica disponível para uso por outros usuários. Quando outro usuário inicia o aplicativo, ele é instalado e o sistema operacional atualiza seu banco de dados AppX para indicar "como instalado" por esse usuário.

Um logoff elegante 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 que permanecem na sessão VDA impedem que ela seja encerrada corretamente. Para resolver isso, determine qual processo está impedindo o encerramento da sessão VDA e, em seguida, adicione-o ao valor da chave de registro "LogoffCheckSysModules", seguindo as orientações em CTX891671.

Os nomes de exibição e as descrições de aplicativos para aplicativos UWP podem não ter os nomes corretos. Edite e corrija essas propriedades ao adicionar os aplicativos ao grupo de entrega.

Verifique Problemas conhecidos para quaisquer problemas adicionais.

Atualmente, vários aplicativos UWP têm ícones brancos com transparência ativada, o que faz com que o ícone não seja visível contra o fundo branco da exibição do StoreFront. Para evitar esse problema, você pode alterar o plano de fundo. Por exemplo, na máquina StoreFront, edite o arquivo `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. No final do arquivo, adicione `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`. O gráfico a seguir ilustra o antes e o depois para este exemplo.



No Windows Server 2016 e versões posteriores, o Gerenciador do Servidor também pode ser iniciado quando um aplicativo UWP é iniciado. Para evitar que isso ocorra, desabilite o Gerenciador do Servidor de iniciar automaticamente durante o logon com a chave de registro `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Para obter detalhes, consulte `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`.

Instalar e publicar aplicativos UWP

O suporte para aplicativos UWP é habilitado por padrão.

Para instalar um ou mais aplicativos UWP em VDAs (ou uma imagem mestre), use um dos seguintes métodos:

- Conclua uma instalação offline da Windows Store for Business, usando uma ferramenta como Deployment Image Servicing and Management (DISM) para implantar os aplicativos na imagem da área de trabalho. Para obter mais informações, consulte Windows Package Manager.

- Faça o sideload dos aplicativos. Para obter mais informações, consulte Sideload de aplicativos de linha de negócios (LOB) em dispositivos cliente Windows.
- Instale os aplicativos UWP para cada usuário pretendido diretamente da Windows Store for Business.

Para adicionar (publicar) um ou mais aplicativos UWP no Citrix Virtual Apps ou Citrix Virtual Desktops™:

1. Depois que os aplicativos UWP forem instalados na máquina, adicione os aplicativos UWP a um grupo de entrega ou grupo de aplicativos. Você pode fazer isso ao criar um grupo ou mais tarde. Na página **Aplicativos**, no menu **Adicionar**, selecione **Do menu Iniciar**.
2. Quando a lista de aplicativos aparecer, selecione os aplicativos UWP que deseja publicar.
3. Continue com o assistente ou feche a caixa de diálogo de edição.

Para obter informações sobre requisitos de configuração adicionais ao usar o User Profile Manager (UPM), consulte Aplicativos Windows - Microsoft Store.

Para desabilitar o uso de aplicativos UWP em um VDA, adicione a configuração de registro **EnableUWASeamlessSupport** em `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` e defina como **0**.

Desinstalar aplicativos UWP

Ao desinstalar 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.

Zonas

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 do SQL Server.

  Esta opção é recomendada para grandes implantações corporativas. Vários sites são gerenciados separadamente, e cada um requer seu próprio banco de dados de site do SQL Server. Cada site é uma implantação separada do Citrix Virtual Apps™.

- Configurar várias zonas dentro de um único site.

  A configuração de zonas pode ajudar os usuários em regiões remotas a se conectarem a recursos sem necessariamente forçar suas conexões a atravessar grandes segmentos da WAN. O uso de zonas permite o gerenciamento eficaz do site a partir de um único console do Citrix 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 Controladores 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 a adição de 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 de 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 de site na zona primária. Além disso, as zonas de failover e preferenciais funcionam de forma diferente nesta versão.

Tipos de zona

Um site sempre tem uma zona primária. Ele também pode, opcionalmente, ter uma ou mais zonas satélite. As zonas satélite podem ser usadas para recuperação de desastres, data centers geograficamente distantes, filiais, uma nuvem ou uma zona de disponibilidade em uma nuvem.

Zona primária:

A zona primária tem o nome padrão "Primary". Esta zona contém o banco de dados do site do SQL Server (e servidores SQL de alta disponibilidade, se usados), Studio, Director, Citrix

StoreFront™, Citrix License Server e Citrix Gateway. Mantenha sempre o banco de dados do site na zona primária.

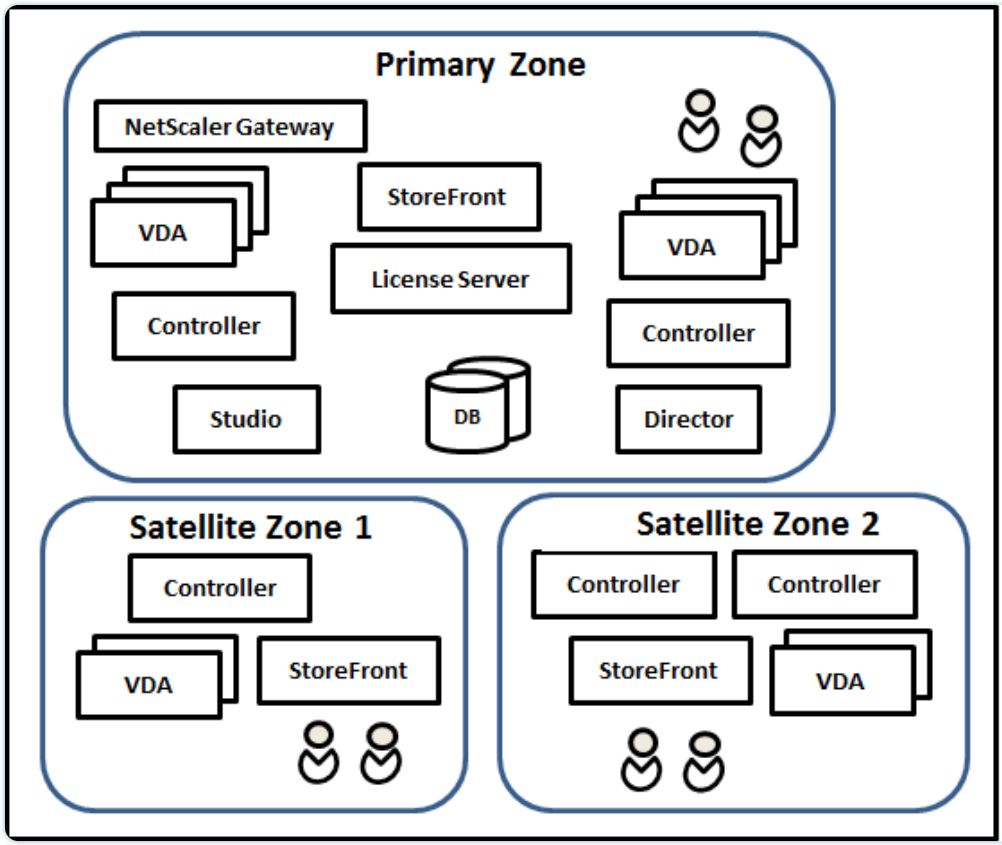
A zona primária deve ter pelo menos dois Controladores para redundância. A zona primária pode ter VDAs com aplicativos que estão fortemente acoplados ao banco de dados e à infraestrutura.

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, 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 Controller na zona satélite continue a intermediar conexões para VDAs nessa zona. Essa implantação pode ser eficaz em um escritório onde os trabalhadores usam um site StoreFront local e o Controller local para acessar seus recursos locais.
- **Zona satélite 2: VDAs com 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 Controller na zona primária. Um VDA na zona primária nunca tenta se registrar em um Controller em uma zona satélite.
- Um VDA em uma zona satélite se registra em um Controller local, se possível. (Este é considerado o Controller preferencial.) Se nenhum Controller local estiver disponível (por exemplo, porque não podem aceitar mais registros de VDA ou falharam), o VDA tentará se registrar em um Controller na zona primária. Nesse caso, o VDA permanece registrado na zona primária, mesmo que um Controller em uma zona satélite volte a ficar disponível. Um VDA em uma zona satélite nunca tenta se registrar em um Controller em outra zona satélite.
- Quando a atualização automática está habilitada para a descoberta de Controllers pelo VDA, e você especifica uma lista de endereços de Controller durante a instalação do VDA, um Controller é selecionado aleatoriamente dessa lista para o registro inicial (independentemente da zona em que o Controller reside). Após a reinicialização da máquina com esse VDA, o VDA começará a preferir se registrar em um Controller em sua zona local.
- Se um Controller em uma zona satélite falhar, ele fará failover para outro Controller local, se possível. Se nenhum Controller local estiver disponível, ele fará failover para um Controller na zona primária.

- Se você mover um Controller para dentro ou para fora de uma zona, e a atualização automática estiver habilitada, os VDAs em ambas as zonas receberão listas atualizadas indicando quais Controllers são locais e quais estão na zona primária, para que saibam com quem podem se registrar e de quem podem aceitar conexões.
- Se você mover um catálogo para outra zona, os VDAs nesse catálogo se registrarão novamente com os Controllers na zona para onde você moveu o catálogo. (Ao mover um catálogo para outra zona, certifique-se de que esta zona e a zona com a conexão de host associada estejam bem conectadas. Se houver largura de banda limitada ou alta latência, mova a conexão de host para a mesma zona que contém o catálogo de máquinas associado.)

Se todos os Controladores na zona primária falharem:

- O 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 Controllers na zona primária se tornem disponíveis.

Para sites que contêm versões de VDA anteriores a 7.7:

- Um VDA em uma zona satélite aceita solicitações de Controllers em sua zona local e na zona primária. (VDAs na versão mínima 7.7 podem aceitar solicitações de Controller de outras zonas satélites.)
- Um VDA em uma zona satélite se registra com um Controller na zona primária ou na zona local aleatoriamente. (VDAs na versão mínima 7.7 preferem a zona local.)

Preferência de zona

Para usar o recurso de preferência de zona, você deve estar usando no mínimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

Em um site multi-zona, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou desktop.

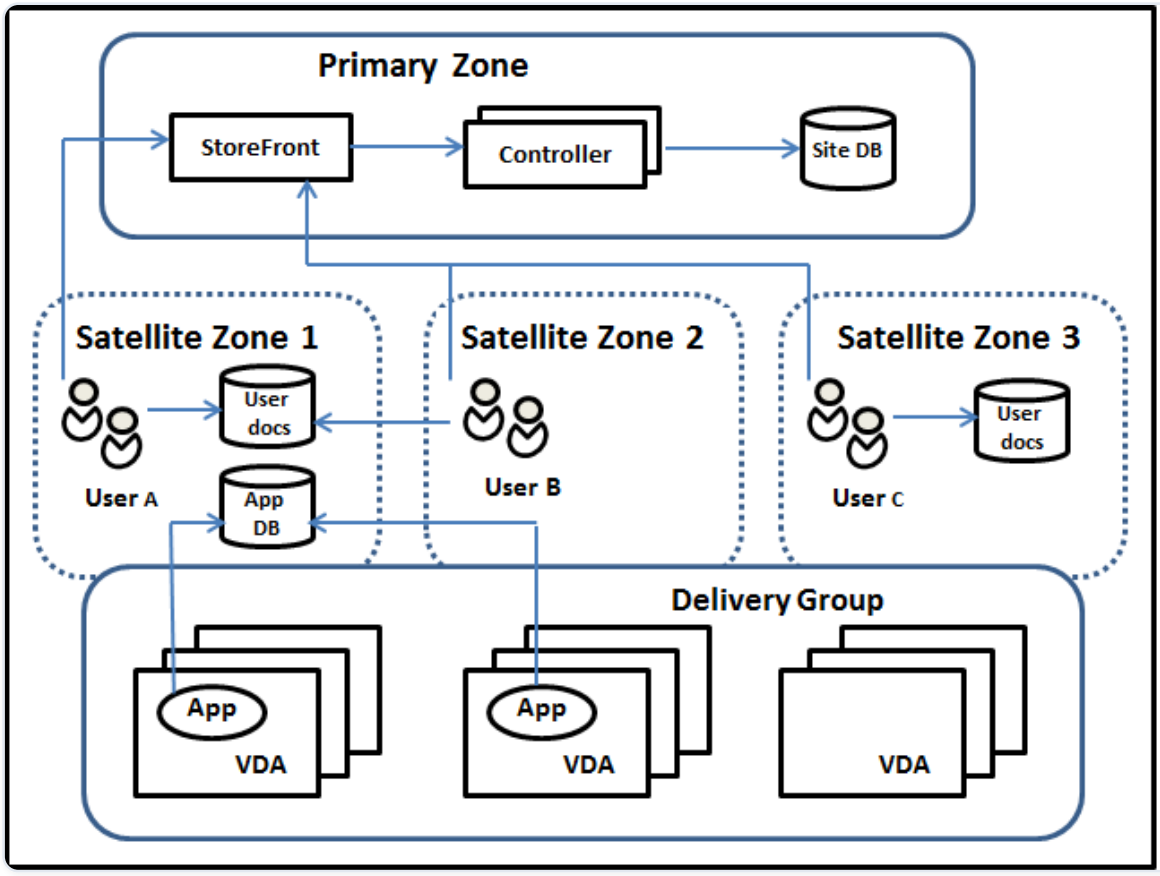
Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma zona específica, com base em:

- Onde os dados do aplicativo são armazenados. Isso é chamado de home do aplicativo.
- O local dos dados home do usuário, como um perfil ou compartilhamento home. Isso é chamado de home do usuário.

- A localização atual do usuário (onde o aplicativo Citrix Workspace™ está sendo executado). Isso é referido como a localização do usuário.

O gráfico a seguir mostra um exemplo de configuração multizona.



Neste exemplo, os VDAs estão distribuídos entre três zonas satélites, mas todos estão no mesmo Grupo de Entrega. Portanto, o broker pode ter uma escolha de qual VDA usar para uma solicitação de inicialização do usuário. Este exemplo indica que existem vários locais onde os usuários podem estar executando seus endpoints do aplicativo Citrix Workspace:

- O Usuário A está usando um dispositivo com o aplicativo Citrix Workspace na zona satélite 1.
- O Usuário B está usando um dispositivo na zona satélite 2.
- Os documentos de um usuário podem ser armazenados em vários locais.
    - Os Usuários A e B usam um compartilhamento baseado na zona satélite 1.
    - O Usuário C usa um compartilhamento da zona satélite C.
    - Um dos aplicativos publicados usa um banco de dados localizado na zona satélite 1.

Você associa um usuário ou aplicativo a uma zona configurando uma zona inicial para o usuário ou aplicativo. O broker no Delivery Controller™ então usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se houver recursos disponíveis. Você pode:

- Configure a zona home para um usuário adicionando um usuário a uma zona.
- Configure a zona inicial para um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona inicial por vez. (Uma exceção para usuários pode ocorrer quando várias associações de zona ocorrem devido à associação a grupos de usuários; consulte a seção "Outras considerações". No entanto, mesmo neste caso, o broker usa apenas uma zona inicial.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o broker seleciona apenas uma zona preferencial para um lançamento. A ordem de prioridade padrão para selecionar a zona preferencial é zona inicial do aplicativo \> zona inicial do usuário \> localização do usuário. Você pode restringir a sequência; consulte Personalizando a preferência de zona. Quando um usuário inicia um aplicativo:

- Se essa aplicação tiver uma associação de zona configurada (uma zona inicial da aplicação), então a zona preferencial é a zona inicial para essa aplicação.
- Se o aplicativo não tiver uma associação de zona configurada, mas o usuário tiver uma associação de zona configurada (uma zona inicial do usuário), então a zona preferencial é a zona inicial para esse usuário.
- Se nem o aplicativo nem o usuário tiverem uma associação de zona configurada, então a zona preferencial é a zona onde o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, uma seleção aleatória de VDA e zona é usada. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver zona preferencial, o balanceamento de carga é aplicado a todos os VDAs no Delivery Group.

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 Delivery Group, você pode especificar que uma sessão seja iniciada 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 deve 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 apenas nessa zona,

sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona inicial do aplicativo.

- **Nenhuma zona inicial de aplicativo e ignorar a zona inicial de usuário configurada:** Se você não especificar uma zona inicial para um aplicativo, também poderá indicar que nenhuma zona de usuário configurada deve ser considerada ao iniciar esse aplicativo. Por exemplo, você pode preferir que os usuários executem um aplicativo em um VDA próximo ao seu dispositivo, usando a preferência de zona de localização do usuário, mesmo que alguns usuários possam ter uma zona inicial diferente.

Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia uma aplicação ou desktop, o broker prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário que inicia um aplicativo ou desktop já tiver uma sessão adequada para o recurso que está sendo iniciado (por exemplo, que possa usar o compartilhamento de sessão para um aplicativo, ou uma sessão que já esteja executando o recurso que está sendo iniciado), mas essa sessão estiver sendo executada em um VDA em uma zona diferente da zona preferencial para o usuário/aplicativo, então o sistema poderá criar uma nova sessão. Isso satisfaz o lançamento na zona correta (se tiver capacidade disponível), antes de reconectar a uma sessão em uma zona menos preferencial para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não pode mais ser alcançada, a reconexão é permitida para sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem de desejabilidade para as sessões satisfazerem um lançamento é:

1. Reconectar a uma sessão existente na zona preferencial.
2. Reconectar a uma sessão desconectada existente em uma zona diferente da zona preferencial.
3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar a uma sessão conectada existente em uma zona diferente da zona preferencial.
5. Iniciar uma nova sessão em uma zona diferente da zona preferencial.

Outras considerações sobre a preferência de zona

- Se você configurar uma zona inicial para um grupo de usuários (como um grupo de segurança), os usuários desse grupo (por meio de associação direta ou indireta) serão associados à zona especificada. No entanto, um usuário pode ser membro de vários grupos de segurança e, portanto, pode ter uma zona inicial diferente configurada por meio de outra

associação de grupo. Nesses casos, a determinação da zona inicial desse usuário pode ser ambígua.

Se um usuário tiver uma zona inicial configurada que não foi adquirida por meio de associação a grupo, essa zona será usada para preferência de zona. Quaisquer associações de zona adquiridas por meio de associação a grupo são ignoradas.

Se o usuário tiver várias associações de zona diferentes adquiridas exclusivamente por meio da associação a grupos, o broker escolherá aleatoriamente entre as zonas. Uma vez que o broker faça essa escolha, essa zona será usada para lançamentos de sessão subsequentes, até que a associação a grupos do usuário mude.

- A preferência de zona de localização do usuário requer a detecção do Citrix Workspace app no dispositivo de endpoint pelo Citrix Gateway através do qual esse dispositivo está se conectando. O Citrix Gateway deve ser configurado para associar intervalos de endereços IP a zonas específicas, e a identidade da zona descoberta deve ser passada através do StoreFront para o Controller.

Para obter mais informações sobre a preferência de zona, consulte Detalhes internos da preferência de zona.

Considerações, requisitos e melhores práticas

- Você pode colocar os seguintes itens em uma zona: Controllers, catálogos de máquinas, conexões de host, usuários e aplicativos. Se um catálogo usar uma conexão de host, certifique-se de que o catálogo e a conexão estejam na mesma zona. (No entanto, com uma conexão de baixa latência e alta largura de banda disponível, eles podem estar em zonas diferentes.)
- Quando você coloca itens em uma zona satélite, isso afeta como o site interage com eles e com outros objetos relacionados a eles.
    - Quando os Controllers são colocados em uma zona satélite, presume-se que essas máquinas tenham boa conectividade (local) com os hipervisores e VDAs na mesma zona. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária para lidar com esses hipervisores e máquinas VDA.
    - Quando uma conexão de hipervisor é colocada em uma zona satélite, presume-se que todos os hipervisores gerenciados por meio dessa conexão de hipervisor também residam nessa zona satélite. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária ao se comunicar com essa conexão de hipervisor.

    - Quando um catálogo de máquinas é colocado em uma zona satélite, presume-se que todas as máquinas VDA nesse catálogo estejam na zona satélite. Os Controllers locais são usados em preferência aos Controllers na zona primária ao tentar se registrar no site, depois que o mecanismo de atualização automática da lista de Controllers for ativado após o primeiro registro de cada VDA.
    - As instâncias do Citrix Gateway também podem ser associadas a zonas. Isso é feito como parte da configuração de Roteamento HDX™ Otimizado do StoreFront, e não, como para os outros elementos descritos aqui, como parte da configuração do site. Quando um Citrix Gateway é associado a uma zona, ele é preferencialmente usado quando as conexões HDX para máquinas VDA nessa zona são utilizadas.

- Quando você cria um site de produção e, em seguida, cria o primeiro catálogo e Grupo de Entrega, todos os itens estão na zona primária – você não pode criar zonas satélite até que conclua 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 a exibição do Studio indique qual zona é a zona primária, é uma prática recomendada usar um nome facilmente identificável para a zona primária. Você pode reatribuir a zona primária (ou seja, tornar outra zona a zona primária), mas ela deve sempre conter o banco de dados do site e quaisquer servidores de alta disponibilidade.
- Sempre mantenha o banco de dados do site na zona primária.
- Depois de criar uma zona, você pode mover itens de uma zona para outra. Essa flexibilidade permite que você separe itens que funcionam melhor em proximidade. Por exemplo, mover um catálogo para uma zona diferente da conexão (host) que cria as máquinas no catálogo, pode afetar o desempenho. Considere os possíveis efeitos não intencionais antes de mover itens entre zonas. Mantenha um catálogo e a conexão de host que ele usa na mesma zona, ou em zonas bem conectadas (por exemplo, por meio de uma rede de baixa latência e alta largura de banda).
- Para um desempenho ideal, instale o Studio e o Director apenas na zona primária. Se você quiser outra instância do Studio em uma zona satélite (por exemplo, uma zona satélite contendo Controllers para usar como failover se a zona primária se tornar inacessível), execute o Studio como um aplicativo publicado localmente. Você também pode acessar o Director de uma zona satélite porque é um aplicativo 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 de intermediação

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 fazem, 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, atrasos extras ocorrem enquanto o processo de intermediação 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 de 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 o Citrix Provisioning™: O console do Citrix Provisioning não reconhece zonas, então a Citrix recomenda usar o Studio para criar catálogos para zonas satélite. Crie o catálogo no 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 terá que usar o Studio para movê-lo para a zona satélite mais tarde.)

Criar uma zona

1. Selecione **Configuração \> Zonas** no painel de navegação do Studio.
2. Selecione **Criar Zona** no painel Ações.
3. Insira um nome para a zona e uma descrição (opcional). O nome deve ser exclusivo dentro do site.
4. 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.
5. Clique em **Salvar**.

Como alternativa a este método, você pode selecionar um ou mais itens no Studio e, em seguida, selecionar **Criar Zona** no painel Ações.

Alterar um nome ou descrição de zona

1. Selecione **Configuração \> Zonas** no painel de navegação do Studio.
2. Selecione uma zona no painel central e, em seguida, selecione **Editar Zona** no painel Ações.
3. Altere o nome da zona, a descrição ou ambos. Se você alterar o nome da zona primária, certifique-se de que a zona permaneça facilmente identificável como a zona primária.
4. Clique em **OK** ou **Aplicar**.

Mover itens de uma zona para outra

1. Selecione **Configuração \> Zonas** no painel de navegação do Studio.
2. Selecione uma zona no painel do meio e, em seguida, selecione um ou mais itens.
3. Arraste os itens para a zona de destino ou selecione **Mover Itens** no painel 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. Selecione **Configuração \> Zonas** no painel de navegação do Studio.
2. Selecione uma zona no painel do meio.
3. Selecione **Excluir Zona** no painel Ações. Se a zona não estiver vazia (contiver itens), será solicitado que você escolha a zona para onde esses itens serão movidos.
4. 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. Selecione **Configuração \> Zonas** no painel de navegação do Studio e, em seguida, selecione uma zona no painel do meio.
2. Selecione **Adicionar Usuários à Zona** no painel Ações.
3. 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 oferecerá duas opções: **Sim** = adicionar apenas os usuários especificados que não têm uma zona inicial; **Não** = retornar à caixa de diálogo de seleção de usuário.
4. Clique em **OK**.

Para usuários com uma zona inicial configurada, você pode exigir que as sessões sejam iniciadas apenas a partir de sua zona inicial:

1. Crie ou edite um Grupo de Entrega.
2. Na página **Usuários**, marque a caixa de seleção **As sessões devem ser iniciadas na zona inicial de um usuário, se configurado**.

Todas as sessões iniciadas por um usuário nesse Grupo de Entrega devem ser iniciadas a partir de máquinas na zona inicial desse usuário. Se um usuário no Grupo de Entrega não tiver uma zona inicial configurada, essa configuração não terá efeito.

Remover uma zona inicial para um usuário

Este procedimento também é conhecido como remover um usuário de uma zona.

1. Selecione **Configuração \> Zonas** no painel de navegação do Studio e, em seguida, selecione uma zona no painel central.
2. Selecione **Remover Usuários da Zona** no painel Ações.
3. 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.
4. Confirme a remoção quando solicitado.

Gerenciar zonas de origem para aplicativos

Configurar uma zona de origem 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 de origem.

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 for adicionado, selecione **Aplicativos** no painel de navegação do Studio. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** no painel 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, marque a caixa de seleção abaixo do botão de opção. Neste caso, nem as zonas de aplicativo nem as zonas iniciais do usuário são usadas para determinar onde iniciar este aplicativo.

Outras ações que incluem a especificação de zonas

Depois de criar pelo menos uma zona satélite, você pode especificar uma zona ao adicionar uma conexão de host ou criar um catálogo.

Normalmente, a zona primária é a padrão. Ao usar o Machine Creation Services™ para criar um catálogo, a zona configurada para a conexão 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.

Conexões e recursos

Importante:

A partir do Citrix Virtual Apps and Desktops™ 7 2006, se sua implantação atual usa alguma das seguintes tecnologias, você pode 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.

Se você deseja usar conexões de host de nuvem pública em 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, e uma mensagem explicativa aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Efeito da Licença de Direitos Híbridos na conexão de host

Existem três cenários onde a conexão de host com os hosts de nuvem pública é afetada com base no direito à Licença de Direitos Híbridos:

- Para criar uma nova conexão de host com os hosts de nuvem pública, você deve ter uma Licença de Direitos Híbridos.
- Se você tem a Licença de Direitos Híbridos, mas a licença expirou, então as conexões existentes com os hosts de nuvem pública são marcadas como não autorizadas e entram em modo de manutenção. Quando as conexões de host existentes estão em modo de manutenção, você não pode fazer o seguinte:
  - Adicionar ou modificar conexões de host
  - Criar catálogo e atualizar imagem
  - Executar ações de energia
- Quando as conexões de host não autorizadas mudam para autorizadas, as conexões de hospedagem existentes são reativadas.

Introdução

Você pode, opcionalmente, criar sua primeira conexão com os recursos de hospedagem ao criar um Site. Mais tarde, 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:

- **Citrix Hypervisor™ (anteriormente XenServer):**
  - Ambientes de virtualização do Citrix Hypervisor.
  - Documentação do Citrix Hypervisor.

- **Nutanix Acropolis:**
  - Ambientes de virtualização Nutanix.
  - Documentação do Nutanix.
- **VMware:**
  - Ambientes de virtualização VMware(/pt-br/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare/vmware.html).
  - Documentação do produto VMware.
- **Microsoft Hyper-V:**
  - ambientes de virtualização do Microsoft System Center Virtual Machine Manager](/pt-br/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare/msscvmm.html) artigo.
  - Documentação da Microsoft.
- **Conexões de host de nuvem pública (AWS, Microsoft Azure, Google Cloud):** 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 Citrix DaaS, a interface de gerenciamento é conhecida como Configuração Completa. No Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Citrix Studio. As atualizações são lançadas para o serviço aproximadamente a cada quatro semanas. Portanto, você pode descobrir que certos recursos disponíveis com o serviço não estão disponíveis na versão local.

Armazenamento do host

Um produto de armazenamento é suportado quando gerenciado por um hipervisor suportado. O Suporte Citrix auxilia esses fornecedores de produtos de armazenamento na solução 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 dispositivo de um fornecedor de armazenamento. O armazenamento central também pode fornecer suas próprias otimizações, como caminhos de controle de armazenamento do hipervisor e acesso direto 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 Citrix Hypervisor para armazenamento de dados temporários, 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 de nome.)

Armazenamento compartilhado por hipervisores

O método de armazenamento compartilhado por hipervisores armazena dados que precisam de persistência de longo prazo de forma centralizada, fornecendo backup e gerenciamento centralizados. Esse armazenamento contém os discos do SO.

Ao selecionar este método, você pode escolher se deseja usar armazenamento local (em servidores no mesmo pool de hipervisores) para dados temporários da máquina. Este método não requer persistência ou tanta resiliência quanto os dados no armazenamento compartilhado, conhecido como *cache de dados temporários*. O disco local ajuda a reduzir o tráfego para o armazenamento principal do SO. Este disco é limpo após cada reinício da máquina. O disco é acessado através de um cache de memória write-through. Se você usar armazenamento local para dados temporários, o VDA provisionado estará vinculado a um host hipervisor específico. Se esse host falhar, a VM não poderá iniciar.

Exceção: O Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários em armazenamento local ao usar Volumes de Armazenamento Clusterizados (CSV).

Crie uma conexão para armazenar dados temporários localmente e, em seguida, habilite e configure valores não padrão para o tamanho do disco de cache e o tamanho da memória de cada VM. Os valores padrão são adaptados ao tipo de conexão e são suficientes para a maioria dos casos. Para obter detalhes, consulte Criar catálogos de máquinas.

O hipervisor também pode fornecer tecnologias de otimização por meio do cache de leitura das imagens de disco localmente. Por exemplo, o Citrix Hypervisor 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.

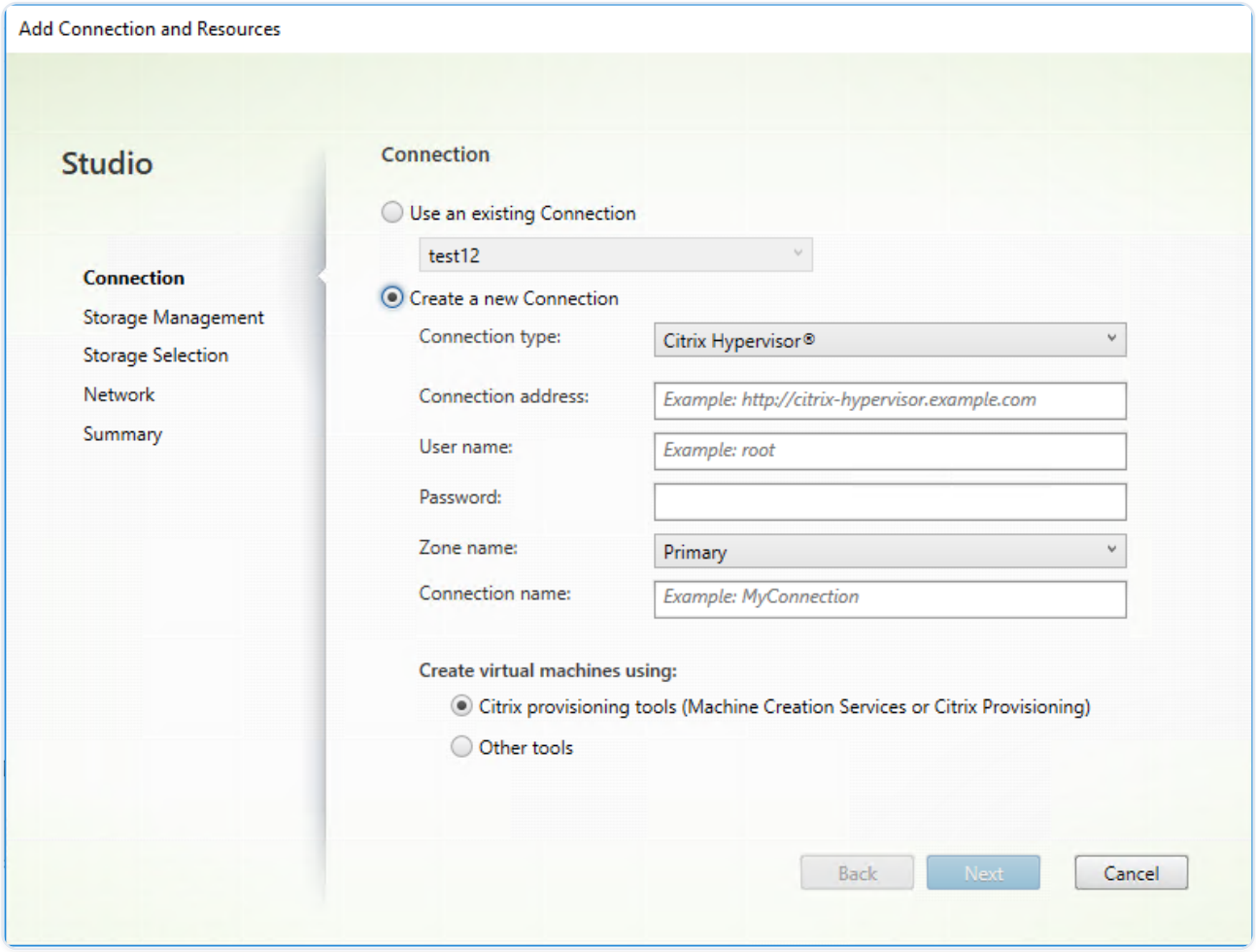
Se você estiver criando uma conexão depois de criar o Site, comece com a etapa 1.

> **Importante:**

> Os recursos do host (armazenamento e rede) devem estar disponíveis antes de você criar uma conexão.

1. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione **Adicionar Conexões e Recursos** no painel **Ações**.
3. 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

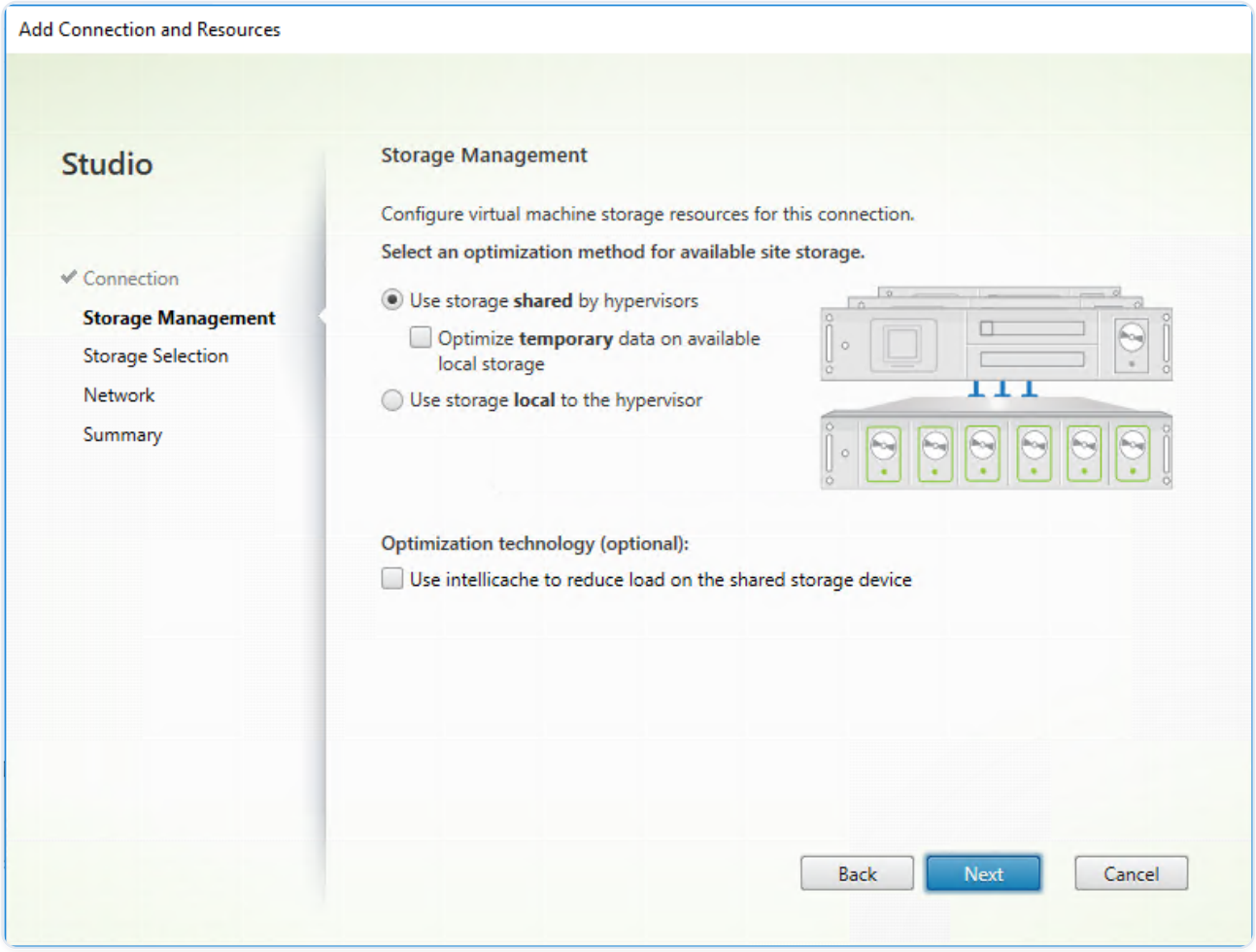


Na página **Conexão**:

- 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.

- 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 Studio.
- Escolha a ferramenta que você usa para criar máquinas virtuais: ferramentas do 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 essa conexão.)

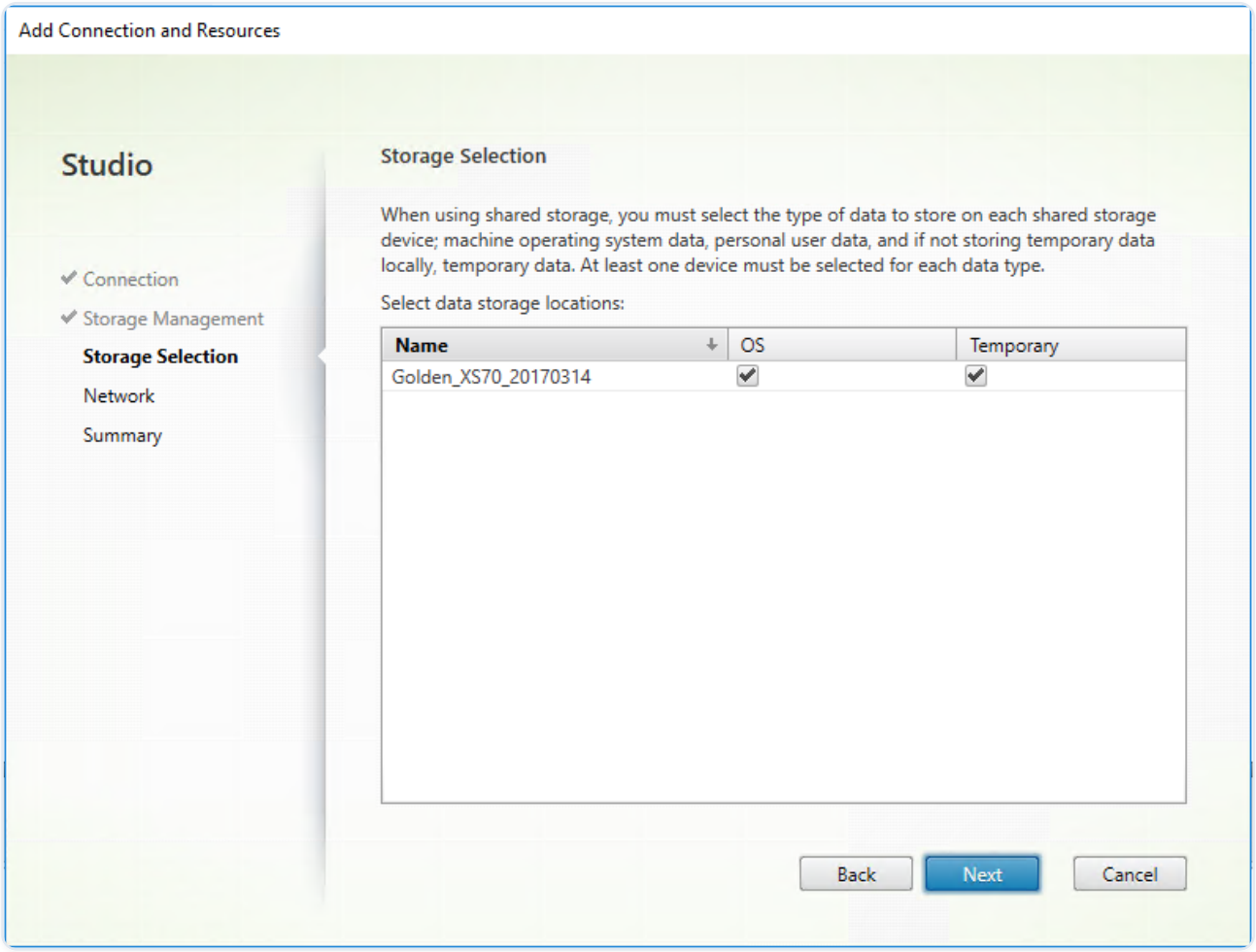
Exceção: Ao usar Clustered Storage Volumes (CSV), o Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários no armazenamento local. A configuração desse gerenciamento de armazenamento no Studio falha.

Se você usar armazenamento compartilhado em um pool do Citrix Hypervisor, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Usar IntelliCache para conexões do Citrix Hypervisor.

Observação:

Em ambientes de virtualização XenServer®, VMware e SCVMM, você pode ter o disco de cache de write-back (WBC) no mesmo local de armazenamento do disco do SO. Para isso, não selecione **Otimizar dados temporários no armazenamento local disponível**.

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 compatível antes de prosseguir para a próxima página do assistente.

> **Nota:**
>
> Em ambientes de virtualização XenServer, VMware e SCVMM, o MCS coloca o disco de cache de write-back (WBC) no mesmo local de armazenamento que o disco do SO se você configurar a lista de armazenamento de SO disponível da mesma forma que a lista de armazenamento temporário disponível.

> 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 clique em **OK**.

Rede

Na página **Rede**, insira um nome para os recursos. Esse nome aparece no Studio para identificar a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs 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 interrompe 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. Selecione **Configuração \> Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** no painel **Ações**.
3. Siga as orientações para as configurações disponíveis ao editar uma conexão.
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.

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 Citrix Hypervisor, selecione **Editar servidores HA**. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o Citrix Hypervisor se o mestre do pool falhar.

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.

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. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão. Para ativar o modo de manutenção, selecione **Ativar Modo de Manutenção** no painel **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

Excluir uma conexão pode resultar na exclusão de um grande número de máquinas e 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. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão e, em seguida, selecione **Excluir Conexão** no painel **Ações**.
3. 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. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão e, em seguida, selecione **Renomear Conexão** ou **Testar Conexão** no painel **Ações**.

Exibir detalhes da máquina em uma conexão

1. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão e, em seguida, selecione **Exibir Máquinas** no painel **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. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione uma conexão e, em seguida, selecione **Exibir Máquinas** no painel **Ação**.

3. Selecione uma das seguintes opções no painel **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.
Reiniciar	Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a área de trabalho permanecerá em seu estado atual.
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

AÇÃO	DESCRIÇÃO
	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 à força. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar o sistema operacional e dados temporários para VMs que usam uma conexão. Você também pode especificar quais servidores usar para o armazenamento de cada tipo de dado.

1. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione a conexão e, em seguida, selecione **Editar Armazenamento** no painel **Ações**.
3. No painel esquerdo, selecione o tipo de dados: sistema operacional ou temporário.
4. Selecione ou desmarque as caixas de seleção para um ou mais dispositivos de armazenamento para o tipo de dados selecionado.
5. Clique em **OK**.

Cada dispositivo de armazenamento na lista inclui seu nome e status de armazenamento. Os valores de status de armazenamento válidos são:

- **Em uso:** O armazenamento está sendo usado para criar máquinas.
- **Substituído:** O armazenamento está sendo usado apenas para máquinas existentes. Nenhuma máquina nova é adicionada neste armazenamento.
- **Não em uso:** O armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo que está atualmente **Em uso**, seu status muda para **Substituído**. As máquinas existentes continuarão a usar esse dispositivo de armazenamento (e podem gravar dados nele), então é possível que esse local fique cheio mesmo depois de parar de ser usado para criar máquinas.

Excluir, renomear ou testar recursos

1. Selecione **Configuração > Hospedagem** no painel de navegação do **Studio**.
2. Selecione o recurso e, em seguida, selecione a entrada apropriada no painel **Ações**: **Excluir Recursos**, **Renomear Recursos** ou **Testar Recursos**.

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.

Cache de Host Local

Para garantir que o banco de dados do site Citrix Virtual Apps and Desktops esteja sempre disponível, a Citrix recomenda iniciar com uma implantação de SQL Server tolerante a falhas, seguindo as melhores práticas de alta disponibilidade da Microsoft. (Para recursos de alta disponibilidade do SQL Server suportados, consulte Bancos de Dados.) No entanto, problemas e interrupções de rede podem resultar na impossibilidade de os usuários se conectarem aos seus aplicativos ou desktops.

O recurso Local Host Cache permite que as operações de intermediação de conexão em um site continuem quando ocorre uma interrupção. Uma interrupção ocorre quando a conexão entre um

Delivery Controller™ e o banco de dados do site falha em um ambiente Citrix® local. O Local Host Cache é ativado quando o banco de dados do site fica inacessível por 90 segundos.

A partir do XenApp e XenDesktop 7.16, o recurso de leasing de conexão (um recurso de alta disponibilidade predecessor em versões anteriores) foi removido do produto e não está mais disponível.

Conteúdo dos dados

O Local Host Cache inclui as seguintes informações, que são um subconjunto das informações no banco de dados principal:

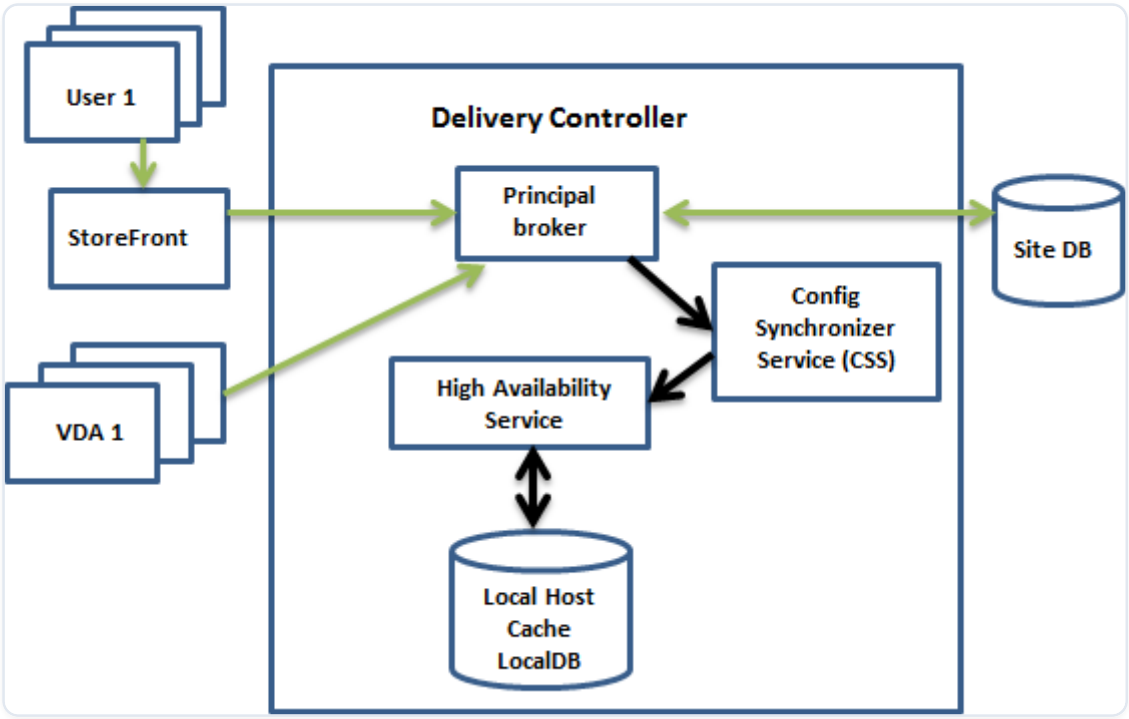
- Identidades de usuários e grupos que têm direitos atribuídos a recursos publicados do site.
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados do site.
- Identidades de máquinas VDA (incluindo máquinas de Acesso Remoto para PC) configuradas no site.
- Identidades (nomes e endereços IP) de máquinas cliente Citrix Receiver™ sendo ativamente usadas para se conectar a recursos publicados.

Ele também contém informações para conexões atualmente ativas que foram estabelecidas enquanto o banco de dados principal estava indisponível:

- Resultados de qualquer análise de endpoint de máquina cliente realizada pelo Citrix Receiver.
- Identidades de máquinas de infraestrutura (como NetScaler Gateway e servidores 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 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 alterar uma propriedade de grupo de entrega) ou ações do sistema (como atribuições de máquina).
- Se uma alteração de configuração ocorreu desde a verificação anterior, o CSS sincroniza (copia) informações para um broker secundário no Controller. (O broker secundário também é conhecido como Serviço de Alta Disponibilidade.)

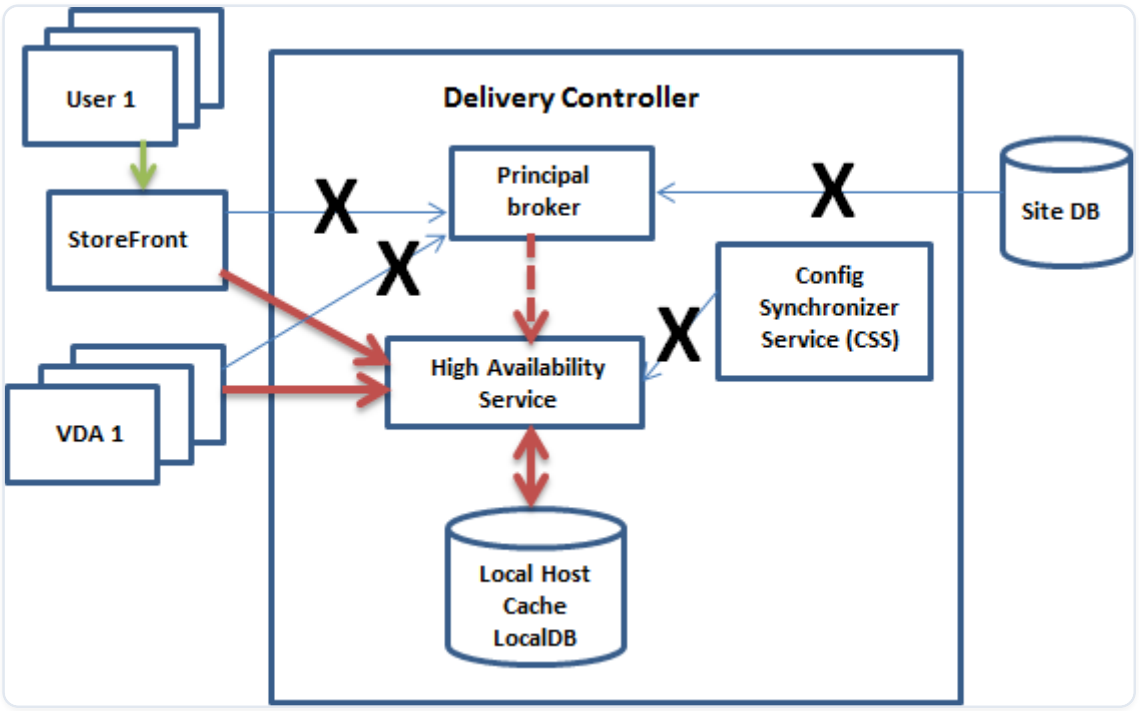
  Todos os dados de configuração são copiados, não apenas os itens que foram alterados desde a verificação anterior. O CSS importa os dados de configuração para um banco de dados Microsoft SQL Server Express LocalDB no Controller. Este banco de dados é referido como o banco de dados Local Host Cache. O 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 a cada sincronização.

  O Microsoft SQL Server Express LocalDB (usado pelo banco de dados Local Host Cache) é instalado automaticamente quando você instala um Controller. (Você pode proibir esta instalação ao instalar um Controller a partir da linha de comando.) O banco de dados Local Host Cache não pode ser compartilhado entre Controllers. Você não precisa fazer backup do

banco de dados Local Host Cache. Ele é recriado toda vez que uma alteração de configuração é detectada.

- Se nenhuma alteração ocorreu desde a última verificação, nenhum dado é copiado.

O gráfico a seguir ilustra as alterações nos caminhos de comunicação se o broker principal perder contato com o banco de dados do site (uma interrupção começa).



Durante uma interrupção

Quando uma interrupção começa:

- O broker secundário começa a escutar e processar 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 brokering. Na próxima vez que um VDA se comunicar com o Brokering Principal, um processo de registro é acionado. O broker secundário remove quaisquer registros VDA restantes da interrupção anterior. O CSS retoma a sincronização de informações quando descobre que ocorreram alterações de configuração na implantação.

No caso improvável de uma interrupção começar durante uma sincronização, a importação atual é descartada e a última configuração conhecida é usada.

O log de eventos fornece informações sobre sincronizações e interrupções.

Não há limite de tempo imposto para operar no modo de interrupção.

A transição entre o modo normal e o modo de interrupção não afeta as sessões existentes. Ela afeta apenas o início 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 conhece todos os brokers secundários pares em execução em outros Controllers na zona.

Os brokers secundários se comunicam entre si em um canal separado. Esses brokers usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual broker secundário será responsável pelas operações de broker na zona se ocorrer uma interrupção. Durante a interrupção, todos os VDAs se registram no broker secundário eleito. Os brokers secundários não eleitos na zona rejeitam ativamente as solicitações de conexão de entrada e de registro de VDA.

Se um broker secundário eleito falhar durante uma interrupção, outro broker secundário é eleito para assumir, e os VDAs se registram com o 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 é eleito, fazendo com que os VDAs se registrem. Depois que o Controller reiniciado é ligado, ele assume automaticamente o brokering, 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:
        - Adicionar uma chave de registro `EnableCssTestMode` com um valor de 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - Usar a porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
    - Depois de executar esses comandos, você pode acessar:
        - Todos os cmdlets `Get-Broker*`.
- As credenciais do hipervisor não podem ser obtidas do Host Service. Todas as máquinas estão no 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 para PC não são possíveis. No entanto, as máquinas que foram registradas e configuradas durante a operação normal são utilizáveis.
- Os usuários de aplicativos e desktops hospedados em servidor 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 somente 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 uma reinicialização agendada para VDAs em um grupo de entrega, as reinicializações começarão quando a

interrupção terminar. Isso pode ter resultados indesejados. Para obter mais informações, consulte Reinicializações agendadas atrasadas devido a interrupção do banco de dados.

- Preferência de zona não pode ser configurada. Se configuradas, as preferências não são consideradas para o lançamento da sessão.
- Restrições de tags, onde as tags são usadas para designar zonas, não são suportadas para lançamentos de sessão. Quando tais restrições de tags 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 Local Host Cache oferece suporte a aplicativos e desktops hospedados em servidor e desktops estáticos (atribuídos).

O Local Host Cache oferece suporte a 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 habilitado 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
  ```

  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 reiniciam automaticamente após a conclusão do

evento LHC. Os VDAs de desktop gerenciados por energia em grupos de entrega agrupados podem reter dados de sessões anteriores até que o VDA seja reiniciado. 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 por um período prolongado 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 capacidade total 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, especialmente 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 apenas um único soquete. Adicionar mais soquetes não melhorará o desempenho (por exemplo, ter 4 soquetes com 1 núcleo cada). Em vez disso, a Citrix recomenda usar vários soquetes com vários núcleos. Em 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 gerencia todas as conexões, então em sites (ou zonas) que fazem balanceamento de carga entre vários Controllers durante operações normais, o broker secundário eleito pode precisar manipular muito mais solicitações do que o normal durante uma interrupção. Portanto, as demandas de CPU serão maiores. Cada broker secundário no site (zona) deve ser capaz de manipular a carga adicional imposta pelo banco de dados do Cache de Host Local 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 "novo" broker secundário adquire informações de sessão de todos os VDAs durante o novo registro) é inevitável. As sessões que estão conectadas quando uma interrupção começa não são

impactadas 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 reduzindo o valor do registro `HeartbeatPeriodMs` do Citrix Broker Protocol (padrão = 600000 ms, que são 10 minutos). Este valor de heartbeat é o dobro do intervalo que o VDA usa para pings, então o valor padrão resulta em um ping a cada 5 minutos.

Por exemplo, o seguinte comando altera o heartbeat para cinco minutos (300000 milissegundos), o que resulta em um ping a cada 2,5 minutos:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Tenha cuidado ao alterar o valor do heartbeat. Aumentar a frequência resulta em maior carga nos Controllers durante os modos normal e de interrupção.

O intervalo não pode ser totalmente eliminado, não importa quão rapidamente os VDAs se registrem.

O tempo necessário para sincronizar entre brokers secundários aumenta com o número de objetos (como VDAs, aplicativos, grupos). Por exemplo, sincronizar 5000 VDAs pode levar 10 minutos ou mais para ser concluído.

Diferenças das versões do XenApp 6.x

Embora esta implementação do 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 `dsmaint` periódicos. Este Local Host Cache é uma implementação tecnicamente diferente.

Gerenciar Cache de Host Local

Para que o Cache de Host Local funcione corretamente, a política de execução do PowerShell em cada Controller deve ser definida como RemoteSigned, Unrestricted ou Bypass.

SQL Server Express LocalDB

O software Microsoft SQL Server Express LocalDB que o Cache de Host Local usa é instalado automaticamente quando você instala um Controller ou atualiza um Controller de uma versão anterior à 7.9. Apenas o broker secundário se comunica com este banco de dados. Você não pode usar cmdlets do PowerShell para alterar nada sobre este banco de dados. O LocalDB não pode ser compartilhado entre Controllers.

O software de banco de dados SQL Server Express LocalDB é instalado independentemente de o Cache de Host Local estar ativado.

Para evitar sua instalação, instale ou atualize o Controller usando o comando `XenDesktopServerSetup.exe` e inclua a opção `/exclude "Local Host Cache Storage (LocalDB)"`. No entanto, lembre-se de que o recurso Cache de Host Local não funcionará sem o banco de dados, e você não pode usar um banco de dados diferente com o broker secundário.

A instalação deste banco de dados LocalDB não tem efeito sobre se você instala o SQL Server Express para uso como banco de dados do site.

Para obter informações sobre como substituir uma versão anterior do SQL Server Express LocalDB por uma versão mais recente, consulte Substituir SQL Server Express LocalDB.

Configurações padrão após a instalação e atualização do produto

Durante uma nova instalação do Citrix Virtual Apps and Desktops (versão mínima 7.16), o Cache de Host Local é ativado.

Após uma atualização (para a versão 7.16 ou posterior), o Cache de Host Local é ativado se houver menos de 10.000 VDAs em toda a implantação.

Ativar e desativar o Cache de Host Local

- Para ativar o Cache de Host Local, 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 leasing de conexão (o recurso que precedeu o Local Host Cache a partir da versão 7.6) foi removido do produto e não está mais disponível.

Verificar se o Local Host Cache está funcionando

Para verificar se o Local Host Cache está configurado e funcionando corretamente:

- Certifique-se de que as importações de sincronização sejam concluídas com êxito. Verifique os logs de eventos.
- Certifique-se de que o banco de dados SQL Server Express LocalDB foi criado em cada Delivery Controller. Isso confirma que o broker secundário pode assumir o controle, se necessário.
  - No servidor Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
  - Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.
- Force uma interrupção nos Delivery Controllers. Depois de verificar se o Local Host Cache funciona, lembre-se de colocar todos os Controllers de volta no modo normal. Isso pode levar aproximadamente 15 minutos.

Logs de eventos

Os logs de eventos indicam quando ocorrem sincronizações e interrupções. Nos logs do visualizador de eventos, o modo de interrupção é referido como *modo HA*.*

Serviço de Sincronização de Configuração:

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados do Local Host Cache usando o broker do Local Host Cache.

- 503: O Serviço de Sincronização de Configuração do Citrix recebeu uma configuração atualizada. Este evento indica o início do processo de sincronização.
- 504: O Serviço de Sincronização de Configuração do Citrix importou uma configuração atualizada. A importação da configuração foi concluída com êxito.

- 505: O Serviço de Sincronização de Configuração do Citrix falhou em uma importação. A importação da configuração não foi concluída com êxito. Se uma configuração bem-sucedida anterior estiver disponível, ela será usada se ocorrer uma interrupção. No entanto, ela estará desatualizada em relação à configuração atual. Se não houver nenhuma configuração anterior disponível, o serviço não poderá participar do balanceamento de sessão durante uma interrupção. Nesse 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 Cache de Host Local está sendo usado para o brokering. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque ocorreu uma interrupção. Este é o comportamento esperado.
- 510: Nenhum dado de configuração do Serviço de Configuração recebido do Serviço de Configuração primário.
- 517: Houve um problema de comunicação com o Broker primário.
- 518: O script de Sincronização de Configuração foi abortado porque o Broker secundário (Serviço de Alta Disponibilidade) não está em execução.

Serviço de Alta Disponibilidade:

Este serviço também é conhecido como broker do Cache de Host Local.

- 3502: Ocorreu uma interrupção e o broker do Cache de Host Local está realizando operações de brokering.
- 3503: Uma interrupção foi resolvida e as operações normais foram retomadas.
- 3504: Indica qual agente de Cache de Host Local é eleito, além de outros agentes de Cache de Host Local envolvidos na eleição.

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 Cache de Host Local a entrar no modo de interrupção, independentemente do estado do banco de dados. Definir o valor como `0` tira o broker do Cache de Host Local do modo de interrupção.

Para verificar eventos, monitore o arquivo de log `Current_HighAvailabilityService` em `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

Solução de problemas

Várias ferramentas de solução de problemas estão disponíveis quando uma importação de sincronização para o banco de dados do Local Host Cache falha e um evento 505 é postado.

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 causa o erro. Este recurso de relatório afeta a velocidade de sincronização, então a Citrix recomenda desativá-lo quando não estiver em uso.

Para habilitar e produzir um relatório de rastreamento CSS, digite o seguinte comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

O relatório HTML é postado 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 agente: Fornece a configuração exata para fins de depuração.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Por exemplo, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

IP virtual e loopback virtual

> **Importante:**

> O Windows 10 Enterprise multi-session não oferece suporte à Virtualização de IP de Área de Trabalho Remota (IP Virtual) e não oferecemos suporte a IP Virtual nem a loopback virtual no Windows 10 Enterprise multi-session.

> Os recursos de IP virtual e loopback virtual são suportados em máquinas Windows Server 2016. Esses recursos não se aplicam a máquinas com sistema operacional Windows desktop.

O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem de comunicações com localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo de localhost (127.*).

Certas aplicações, como CRM e Computer Telephony Integration (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros propósitos que exigem um endereço IP ou endereço de loopback exclusivo. Outras aplicações podem se vincular a uma porta estática, então as tentativas de iniciar instâncias adicionais de uma aplicação em um ambiente multiusuário falham porque a porta está em uso. Para que tais aplicações funcionem corretamente em um ambiente Citrix Virtual Apps™, um endereço IP exclusivo é necessário para cada dispositivo.

IP virtual e loopback virtual são recursos independentes. Você pode usar um ou ambos.

Sinopse da ação do administrador:

- Para usar o IP virtual da Microsoft, habilite-o e configure-o no servidor Windows. (As configurações de política do Citrix® não são necessárias.)
- Para usar o loopback virtual da Citrix, configure duas configurações em uma política da Citrix.

IP virtual

Quando o IP virtual é habilitado e configurado no servidor Windows, cada aplicativo configurado em execução em uma sessão parece ter um endereço exclusivo. Os usuários acessam esses aplicativos em um servidor Citrix Virtual Apps da mesma forma que acessam qualquer outro aplicativo publicado. Um processo requer IP virtual em qualquer um dos seguintes casos:

- O processo usa um número de porta TCP codificado

- O processo usa sockets do Windows e requer um endereço IP exclusivo ou um número de porta TCP especificado

Para determinar se um aplicativo precisa usar endereços IP virtuais:

1. Obtenha a ferramenta TCPView da Microsoft. Esta ferramenta lista todos os aplicativos que vinculam endereços IP e portas específicos.
2. Desative o recurso Resolver Endereços IP para que você veja os endereços em vez dos nomes de host.
3. Inicie a aplicação e use o TCPView para ver quais endereços IP e portas a aplicação 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 uma aplicação não abra o mesmo endereço IP em uma porta diferente, inicie outra instância da aplicação.

Como funciona a virtualização de IP do Microsoft Remote Desktop (RD)

- O endereçamento IP virtual deve ser habilitado no servidor Microsoft.

  Por exemplo, em um ambiente Windows Server 2016, no Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões do Host da Sessão RD** para habilitar o recurso de Virtualização de IP RD e configurar as definições para atribuir dinamicamente endereços IP usando o servidor Dynamic Host Configuration Protocol (DHCP) por sessão ou por programa. Consulte a documentação da Microsoft para obter instruções.
- Após o recurso ser habilitado, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente do servidor DHCP.
- O recurso de Virtualização de IP RD atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilharão um endereço IP por sessão.
- Depois que um endereço é atribuído a uma sessão, a sessão usa o endereço virtual em vez do endereço IP primário para o sistema sempre que as seguintes chamadas são feitas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Ao usar o recurso de virtualização de IP da Microsoft dentro da configuração de hospedagem de sessão de Área de Trabalho Remota, as aplicações são vinculadas a endereços IP específicos inserindo um componente de “filtro” entre a aplicação e as chamadas de função Winsock. A aplicação então vê apenas o endereço IP correto a ser usado. Qualquer tentativa da aplicação de

escutar comunicações TCP ou UDP é vinculada automaticamente ao seu endereço IP virtual alocado (ou endereço de loopback). Quaisquer conexões de origem abertas pela aplicação se originam do endereço IP vinculado à aplicação.

Em funções que retornam um endereço (como `GetAddrInfo()`, que uma política do Windows controla), se o endereço IP do host local for solicitado, o IP virtual examina o endereço IP retornado e o altera para o endereço IP virtual da sessão. Aplicações que tentam obter o endereço IP do servidor local através de tais funções de nome veem apenas o endereço IP virtual exclusivo atribuído a essa sessão. Este endereço IP é frequentemente usado em chamadas de socket subsequentes, como bind ou connect. Para mais informações sobre políticas do Windows, consulte Virtualização de IP RDS no Windows Server.

Frequentemente, um aplicativo solicita vincular-se a uma porta para escutar no endereço 0.0.0.0. Quando um aplicativo faz isso e usa uma porta estática, você não pode iniciar mais de uma instância do aplicativo. O recurso de endereço IP virtual também procura por 0.0.0.0 nesses tipos de chamada e altera a chamada para escutar no endereço IP virtual específico, o que permite que mais de um aplicativo escute na mesma porta no mesmo computador porque todos estão escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço IP virtual estiver habilitado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentarem vincular-se a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas serão vinculadas a VIPAddress1:9000 e VIPAddress2:9000 e não haverá conflito.

Loopback virtual

Habilitar as configurações da política de loopback de IP virtual da Citrix permite que cada sessão tenha seu próprio endereço de loopback para comunicação. Quando um aplicativo usa o endereço localhost (padrão = 127.0.0.1) em uma chamada Winsock, o recurso de loopback virtual simplesmente substitui 127.0.0.1 por 127.X.X.X, onde X.X.X é uma representação do ID da sessão + 1. Por exemplo, um ID de sessão de 7 é 127.0.0.8. No caso improvável de o ID da sessão exceder o quarto octeto (mais de 255), o endereço passa para o próximo octeto (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em qualquer um dos seguintes casos:

- O processo usa o endereço de loopback 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. Este recurso é chamado de loopback preferencial. No entanto, prossiga com cautela:

- Use o loopback preferencial apenas se o IP Virtual e o loopback virtual estiverem habilitados. Caso contrário, você poderá ter resultados indesejados.
- A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Execute regedit nos servidores onde os aplicativos residem.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- Nome: PreferLoopback, Tipo: REG_DWORD, Dados: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dados: \<lista de processos\>

Controladores de Entrega

O Delivery Controller é o componente do lado do servidor responsável por gerenciar o acesso do usuário, além de intermediar e otimizar as conexões. Os Controllers também fornecem os Machine Creation Services™ que criam imagens de desktop e servidor.

Um site deve ter pelo menos um Controller. Depois de instalar o Controller inicial, você pode adicionar mais Controllers ao criar um site ou posteriormente. Há dois benefícios principais em ter mais de um Controller em um site.

- **Redundância:** Como melhor prática, em um site de produção, sempre tenha pelo menos dois Controllers em servidores físicos diferentes. Se um Controller 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 Controller e a atividade do banco de dados. Controllers adicionais permitem que você manipular mais usuários e mais solicitações de aplicativos e desktops, e podem melhorar a capacidade de resposta geral.

Cada Controller se comunica diretamente com o banco de dados do site. Em um site com mais de uma zona, os Controllers 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 Controller depois que o site for configurado.

Como os VDAs se registram nos Controllers

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 Controllers.

Adicionar, remover ou mover Controllers

Para adicionar, remover ou mover um Controller, você deve ter as permissões de função de servidor e função de banco de dados listadas no artigo Bancos de dados.

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

Ao adicionar um Delivery Controller™ a um site, certifique-se de adicionar as credenciais de logon para essa máquina a quaisquer SQL Servers de réplica que você usa para alta disponibilidade.

Se sua implantação usa espelhamento de banco de dados:

- Antes de adicionar, remover ou mover um Controller, certifique-se de que os bancos de dados principal e espelhado estejam 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, inicie o Studio. Você será solicitado a criar um site. Na página Bancos de Dados do assistente de criação de site, clique no botão Selecionar e adicione o endereço do servidor onde você instalou o Controller adicional.

   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, aponte o Studio para o servidor onde você instalou o Controller adicional. Clique em **Dimensionar sua implantação** e insira o endereço do site.

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 Studio.

Ao remover um Controller de um site, o logon do Controller para o servidor de banco de dados não é removido. Isso evita a remoção potencial de um logon que é usado pelos serviços de outros produtos na mesma máquina. O logon deve ser removido manualmente se não for mais necessário. A permissão de função de servidor `securityadmin` é necessária para remover o logon.

Depois de remover um Controller:

- 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 ativado 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 Studio seja carregado em menos de uma hora. Assim que o Studio carregar o Controller que você deseja remover, desligue o Controller quando solicitado.
2. Selecione **Configuração \> Controllers** no painel de navegação do Studio e, em seguida, selecione o Controller que você deseja remover.
3. Selecione **Remover Controller** no painel Ações. 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.

4. 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 Studio para remover um Controller, o tráfego para esse Controller pode persistir por um curto período para garantir a conclusão adequada das tarefas atuais. Se você quiser forçar a remoção de um Controller em pouco tempo, a Citrix recomenda que você desligue o servidor onde ele foi instalado ou remova esse servidor do Active Directory. Em seguida, reinicie os outros Controllers no site para garantir que não haja mais comunicação com o Controller removido.

Mover um Controller para outra zona

Se o seu site contiver mais de uma zona, você poderá mover um Controller para uma zona diferente. Consulte o artigo *Zonas* para obter informações sobre como essa movimentação pode afetar o registro de VDA e outras operações.

1. Selecione **Configuração \> Controllers** no painel de navegação do Studio e, em seguida, selecione o Controller que você deseja mover.
2. Selecione **Mover** no painel Ações.
3. Especifique a zona para a qual você deseja mover o Controller.

Mover um Controller para outro site

Você não pode mover um Controller para um site que foi criado com uma versão anterior deste software.

1. No site onde o Controller está localizado (o site antigo), selecione **Configuration \> Controllers** no painel de navegação do Studio. Em seguida, selecione o Controller que você deseja mover.
2. Selecione **Remove Controller** no painel Ações. Se você não tiver as permissões de banco de dados corretas, poderá gerar um script que permite que alguém com essas permissões (como um administrador de banco de dados) remova o Controller. Um site requer pelo menos um Controller, portanto, você não pode remover o último listado no Studio.
3. No Controller que você está movendo, abra o Studio, redefina os serviços quando solicitado, selecione **Join existing site** e insira o endereço do novo site.

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 no qual foram criados.

Existem duas maneiras de mover um VDA para outro site: usando o instalador ou 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 Delivery Group para iniciar uma migração de VDA em fases entre os sites.
    - Controllers: Contendo FQDNs (entradas DNS) de um ou mais Controllers no site 2.
    - Habilitar atualização automática de Controllers: definido como desabilitado.
2. Cada VDA no Grupo de Entrega é alertado dentro de 90 minutos sobre a nova política. O VDA ignora a lista de Controladores que recebe (porque a atualização automática está desabilitada); ele seleciona um dos Controladores especificados na política, que lista os Controladores no site 2.
3. Quando o VDA se registra com sucesso em um Controlador no site 2, ele recebe o ListOfDDCs do site 2 e as informações da política, que tem a atualização automática habilitada por padrão. O Controlador com o qual o VDA foi registrado no site 1 não está na lista enviada pelo Controlador no site 2. Assim, o VDA se registra novamente, escolhendo entre os Controladores na lista do site 2. A partir de então, o VDA é atualizado automaticamente com informações do site 2.

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 a sincronização de tempo e os problemas de 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 tentará 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 desse cache local, a menos que uma alteração de configuração seja detectada.

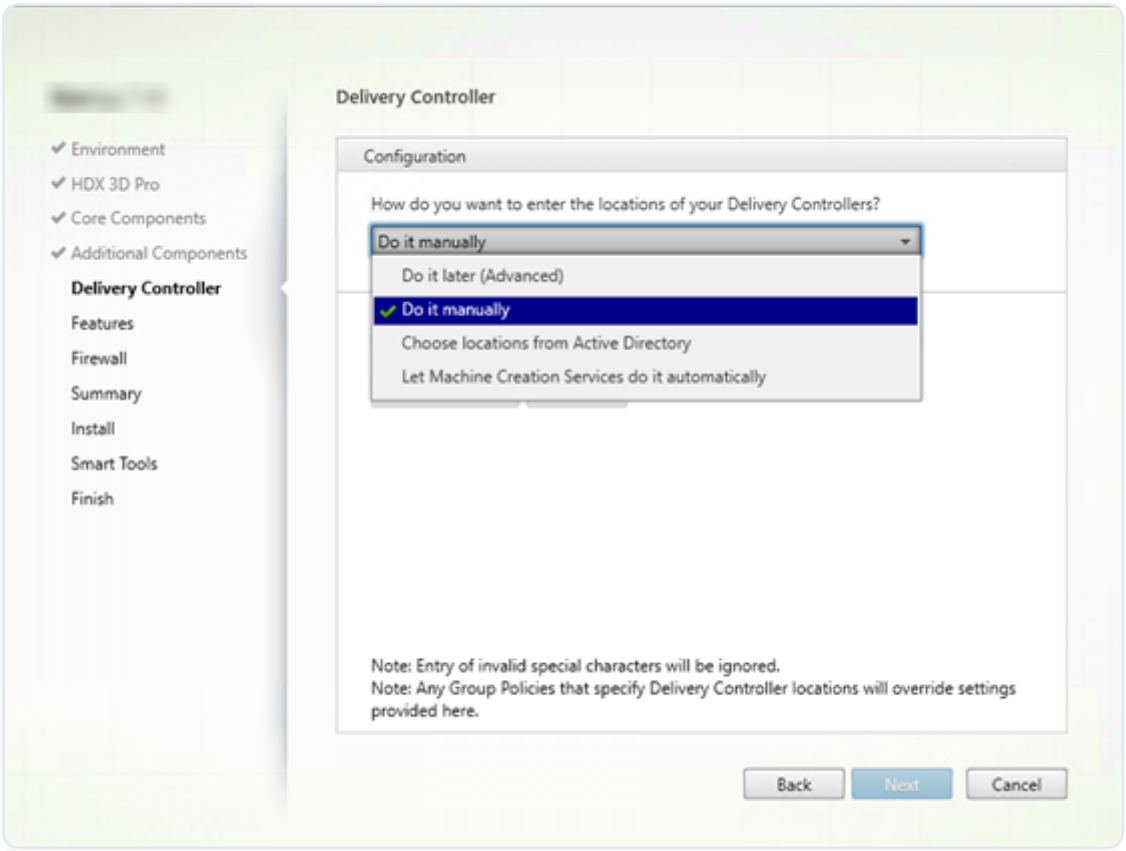
A maneira mais fácil de recuperar essa lista durante registros subsequentes é usando o recurso de atualização automática. A atualização automática é habilitada por padrão. Para mais informações, consulte Atualização automática.

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 UO do Active Directory (descoberta de UO herdada)
- Baseado em MCS (personality.ini)

Você especifica o método de registro inicial ao instalar um VDA. (Se você desativar a atualização automática, o método selecionado durante a instalação do VDA será usado para registros subsequentes.)

O gráfico a seguir mostra a página **Delivery Controller** do assistente de instalação do VDA.



Baseado em política (LGPO\\GPO)

A Citrix® recomenda usar GPO para o registro inicial do VDA. Ele tem a prioridade mais alta. (Embora a atualização automática seja listada como a prioridade mais alta, a atualização automática é usada somente após o registro inicial.) O registro baseado em política oferece as vantagens de centralização do uso da Política de Grupo para configuração.

Para especificar este método, conclua as duas etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer mais tarde (avançado)**. O assistente o lembra várias vezes para especificar os endereços do Controller, mesmo que você não os esteja especificando durante a instalação do VDA. (O registro do VDA é muito importante.)
- Habilite ou desabilite o registro de VDA baseado em política por meio da política Citrix com a configuração `Virtual Delivery Agent Settings > Controllers`. (Se a segurança for sua principal prioridade, use a configuração `Virtual Delivery Agent Settings > Controller SIDs`.)

Essa configuração é armazenada em `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

Baseado em registro

Para especificar este método, conclua uma das seguintes etapas:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer manualmente**. Em seguida, insira o FQDN de um Controller instalado e clique em **Adicionar**. Se você instalou mais Controllers, adicione seus endereços.
- Para uma instalação de VDA por linha de comando, use a opção /controllers e especifique os FQDNs dos Controllers ou Cloud Connectors instalados.

Essa informação é armazenada no valor de registro `ListOfDDCs` na chave de registro `HKLM\Software\Citrix\VirtualDesktopAgent` ou `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

Você também pode configurar esta chave de registro manualmente ou usar 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 da 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` está presente se uma OU de site foi especificada durante a instalação do VDA. (Isso pode ser usado em implantações legadas.)

Opcionalmente, atualize a chave de registro `ListOfSIDs` (para mais informações, consulte ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

Lembre-se: Se você também habilitar o registro de VDA baseado em política através da política Citrix, 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 retroativa 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** no 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.

Para detalhes, consulte descoberta baseada em OU do Active Directory.

Baseado em MCS

Se você usa o MCS para provisionar VMs, o MCS configura a lista de Controladores ou Cloud Connectors. Este recurso funciona com a atualização automática. Ao criar o catálogo, o MCS injeta a lista de Controladores ou Cloud Connectors no arquivo `Personality.ini` durante o provisionamento inicial. A atualização automática mantém a lista atualizada.

Para especificar este método, na página **Delivery Controller** no assistente de instalação do VDA, selecione **Deixar o Machine Creation Services™ fazer isso**.

Revisão e recomendações

Como prática recomendada:

- 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 multi-zona, 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 satélites.
- 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 usada para o registro inicial, o software de atualização automática baixa e armazena o `ListofDDCs` em um cache persistente no VDA quando o registro inicial ocorre. Este processo é feito para cada VDA. O cache também contém informações de política da máquina, o que garante que as configurações de política sejam mantidas após reinicializações.

A atualização automática é suportada ao usar MCS ou Citrix Provisioning™ para provisionar máquinas, exceto para o cache do lado do servidor do Citrix Provisioning. O cache do lado do servidor não é um cenário comum porque não há armazenamento persistente para o cache de atualização automática.

Para especificar esse método:

- Habilite ou desabilite a atualização automática através de uma política Citrix contendo a configuração `Virtual Delivery Agent Settings > Enable auto update of Controllers`. Esta configuração é habilitada por padrão.

Como funciona:

- Cada vez que um VDA se registra novamente (por exemplo, após uma reinicialização da máquina), o cache é atualizado. Cada Controlador ou Cloud Connector também verifica o banco de dados do site a cada 90 minutos. Se um Controlador ou Cloud Connector foi adicionado ou removido desde a última verificação, ou se ocorreu uma alteração de política que afeta o registro do VDA, o Controlador ou Cloud Connector envia uma lista atualizada para seus VDAs registrados e o cache é atualizado. O VDA aceita conexões de todos os Controladores ou Cloud Connectors em sua lista mais recentemente armazenada em cache.

- Se um VDA receber uma lista que não inclui o Controlador ou Cloud Connector com o qual está registrado (em outras palavras, esse Controlador ou Cloud Connector foi removido do site), o VDA se registra novamente, escolhendo entre os Controladores ou Cloud Connectors no `ListofDDCs`.

Exemplo:

- Uma implantação possui três Controladores: A, B e C. Um VDA se registra com o Controlador B (que foi especificado durante a instalação do VDA).
- Posteriormente, dois Controllers (D e E) são adicionados ao site. Em 90 minutos, os VDAs recebem listas atualizadas e, em seguida, aceitam conexões dos Controllers A, B, C, D e E. (A carga não é distribuída igualmente para todos os Controllers 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 originalmente se registrou 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 SIDs 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 de reduzir a carga do Active Directory), 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 for alterado, 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/vrngwl2rc3" 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/9qpt0p609f" 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 Controladores ou Cloud Connectors, a Citrix recomenda usar um endereço FQDN. Um endereço IP não é considerado uma configuração confiável, porque é mais fácil comprometer um IP do que um registro DNS. Se

você preencher o `ListofSIDs` manualmente, poderá usar um IP em um `ListofDDCs`. No entanto, o FQDN ainda é recomendado.

Balanceamento de carga

Conforme observado anteriormente, o VDA distribui automaticamente as conexões entre todos os Controladores ou Cloud Connectors no `ListofDDCs`. A funcionalidade de failover e balanceamento de carga é incorporada ao Citrix Brokering Protocol (CBP). Se você especificar vários Controladores 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 (Controlador). No entanto, o Controlador ou Cloud Connector deve provar sua identidade ao VDA. Isso significa que o VDA e o Controlador 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 Controlador/Cloud Connector e Controlador/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 Controlador 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 reconhecerá corretamente que o IP não pertence ao Controlador ou Cloud Connector esperado.

Para mais informações, consulte:

- Introdução ao Kerberos
- Autenticação mútua usando Kerberos

A atualização automática substitui o CNAME

O recurso de atualização automática substitui a função CNAME (alias DNS) das versões do XenApp e XenDesktop anteriores à 7.x. A funcionalidade CNAME é desabilitada, a partir do XenApp e XenDesktop 7. Use a atualização automática em vez do 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 Controlador/Cloud Connector

Em certos cenários, você pode querer processar Controladores ou Cloud Connectors em grupos, com um grupo sendo preferencial e o outro grupo usado para failover se todos os Controladores/Cloud Connectors falharem. Lembre-se de que os Controladores 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 Controladores/Cloud Connectors. Por exemplo, com quatro Controladores (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 Controladores do primeiro grupo (001 e 002) são processados primeiro. Se ambos falharem, os Controladores 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 Controlador** no Citrix Studio.

ListOfSIDs

A lista de Controllers que um VDA pode contatar para registro é a `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 XML brokers, e XDC-003 e XDC-004 para registro de VDA, você especificava todos os Controllers no `ListofSIDs`, e XDC-003 e XDC-004 no `ListofDDCs`.

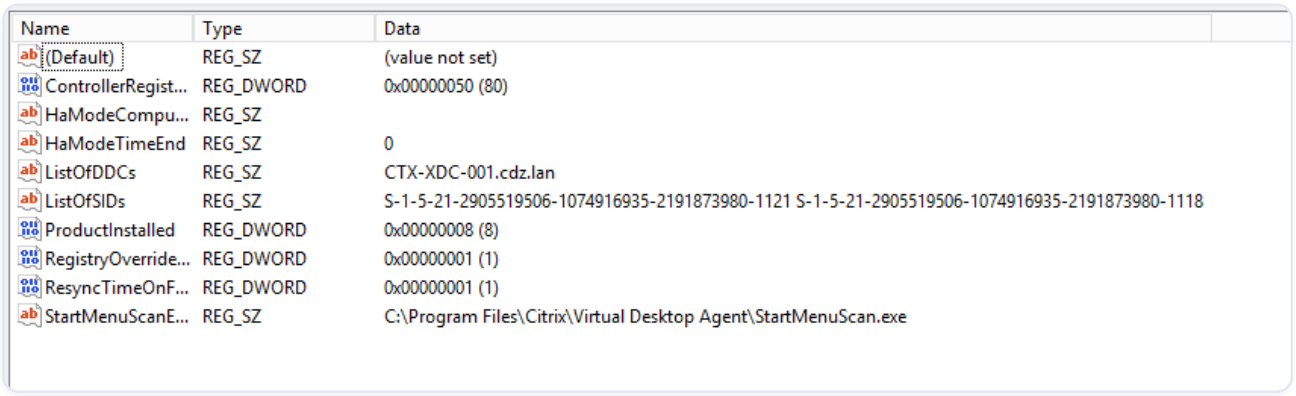
Esta não é uma configuração típica ou recomendada. Não a use em ambientes mais recentes. Em vez disso, use zonas.

- **Reduzindo a carga do Active Directory:** Antes que o recurso de atualização automática fosse introduzido 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, porque este cache persistente contém SIDs. A Citrix recomenda manter o recurso de atualização automática ativado.
- **Segurança:** Em alguns ambientes altamente seguros, os SIDs de Controllers confiáveis eram configurados manualmente para evitar possíveis ameaças de segurança de um servidor DNS comprometido. No entanto, se você fizer isso, também deverá desativar o recurso de atualização automática. Caso contrário, a configuração 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 Agente Broker 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 com frequência. Se o endereço do Controller for inválido (por exemplo, o administrador inseriu um

FQDN incorreto ao instalar o VDA), a atividade dessa consulta pode potencialmente levar a uma condição de negação de serviço distribuída (DDoS) no controlador de domínio.

A seguinte chave de registro controla se o Broker Agent usa a consulta de fallback de cima para baixo quando não consegue localizar um Controller durante a pesquisa inicial.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- Nome: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valor: `0` (padrão) ou qualquer valor diferente de zero

Quando definido como `0`, a pesquisa de fallback é ativada. Se a pesquisa inicial pelo Controller falhar, a pesquisa de fallback de cima para baixo é iniciada. Este é o comportamento padrão. No entanto, se definido como qualquer valor diferente de zero, a pesquisa de fallback é desativada. Se a pesquisa inicial pelo Controller falhar, o Broker Agent para de procurar.

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 Grupo de Entrega.

- **Identificação de 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 foi registrada), você pode optar por adicionar a máquina de qualquer maneira.

  O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto pode exigir um novo VDA. A definição de 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.

- **Identificação de 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 que estão ligadas e não em modo de manutenção, mas que não estão atualmente registradas em um Controller. Ao visualizar uma máquina "não registrada, mas deveria estar", revise a guia **Solução de problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

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.

Gerenciar chaves de segurança

> **Nota:**
>
> Você deve usar este recurso em combinação com o StoreFront™ 1912 LTSR CU2 ou posterior.

> Este recurso permite que apenas máquinas StoreFront e Citrix Gateway aprovadas se comuniquem com os Citrix Delivery Controllers. Depois de habilitar este recurso, todas as solicitações que não contiverem a chave serão bloqueadas. Use este recurso para adicionar uma camada extra de segurança para proteger contra ataques originados da rede interna.

Um fluxo de trabalho geral para usar este recurso é o seguinte:

1. Habilitar o Studio para exibir as configurações do recurso.
2. Configurar as definições para o seu site (Use o console do Studio ou o PowerShell).
3. Configurar as definições no StoreFront (Use o PowerShell).
4. Configurar as definições no Citrix ADC (Use o PowerShell).

Habilitar o Studio para mostrar as configurações do recurso

Por padrão, as configurações das chaves de segurança estão ocultas no Studio. Para habilitar o Studio a exibi-las, use o SDK do PowerShell da seguinte forma:

Para habilitar o recurso, execute estas etapas:

1. Execute o SDK do PowerShell Remoto do Citrix Virtual Apps and Desktops™.
2. Em uma janela de comando, execute os seguintes comandos:
   - `Add-PSSnapIn Citrix*`. Este comando adiciona os snap-ins do Citrix.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

Para obter mais informações sobre o SDK do PowerShell Remoto, consulte SDKs e APIs.

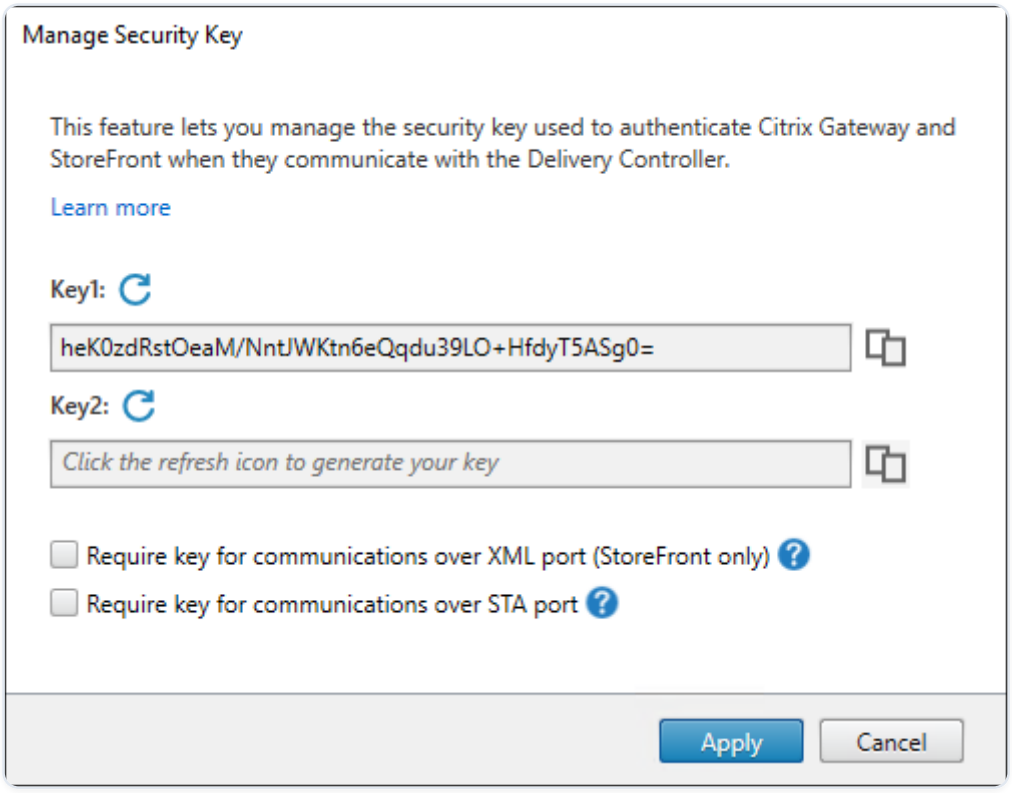
Configurar as definições para o seu site

Você pode configurar as definições no Studio usando o console do Studio ou o PowerShell.

Usar o console do Studio

Depois de habilitar o Studio para mostrar as configurações do recurso, vá para **Studio > Configuration > Manage Security Key**. Pode ser necessário clicar em **Refresh** para que a opção **Manage Security Key** apareça.

A janela **Manage Security Key** aparece depois que você clica em **Manage Security Key**.



Importante:

- Existem duas chaves disponíveis para uso. Você pode usar a mesma chave ou chaves diferentes para comunicações pelas portas XML e STA. Recomendamos que você use apenas uma chave por vez. A chave não utilizada é usada apenas para rotação de chaves.
- Não clique no ícone de atualização para atualizar a chave já em uso. Se o fizer, ocorrerá interrupção do serviço.

Clique no ícone de atualização para gerar novas chaves.

Exigir chave para comunicações pela porta XML (somente StoreFront). Se selecionado, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta XML, consulte o artigo da Central de Conhecimento CTX127945.

Exigir chave para comunicações pela porta STA. Se selecionado, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta STA, consulte o artigo da Central de Conhecimento CTX101988.

Depois de aplicar suas alterações, clique em **Close** para sair da janela **Manage Security Key**.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações do 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 no StoreFront

Após concluir a configuração no Studio, você precisa configurar as definições relevantes no StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos PowerShell:

Para configurar a chave para comunicações pela porta XML, use o comando . Por exemplo:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Insira os valores apropriados para os seguintes parâmetros:

- `Path to store`
- `Resource feed name`
- `secret`

Para configurar a chave para comunicações sobre a porta STA, use os comandos `New-STFSecureTicketAuthority` e `Set-STFRoamingGateway`. Por exemplo:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Insira os valores apropriados para os seguintes parâmetros:

- `Gateway name`
- `STA URL`
- `Secret`

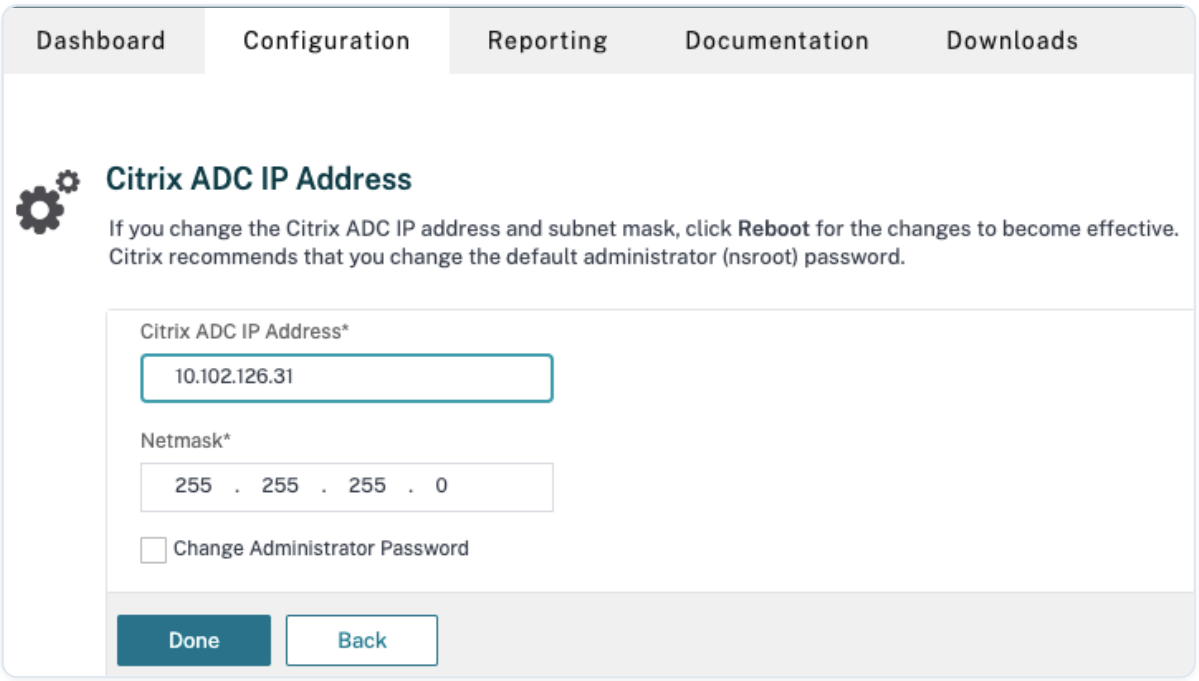
Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

Configurar definições no Citrix ADC

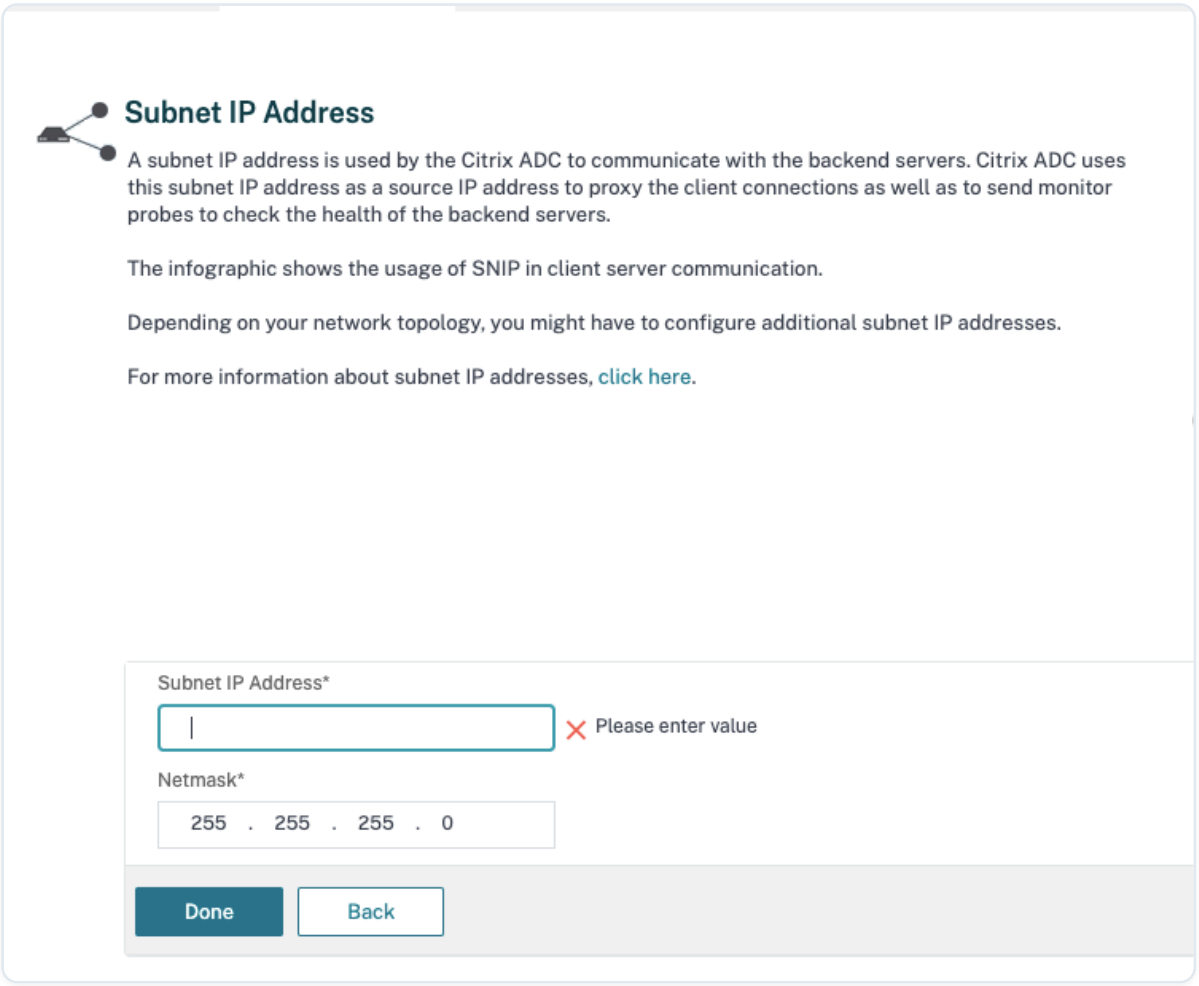
> **Nota:**

> A configuração desse recurso no Citrix ADC não é necessária, a menos que você use o Citrix ADC como seu gateway. Se você usar o Citrix ADC, siga as etapas abaixo.

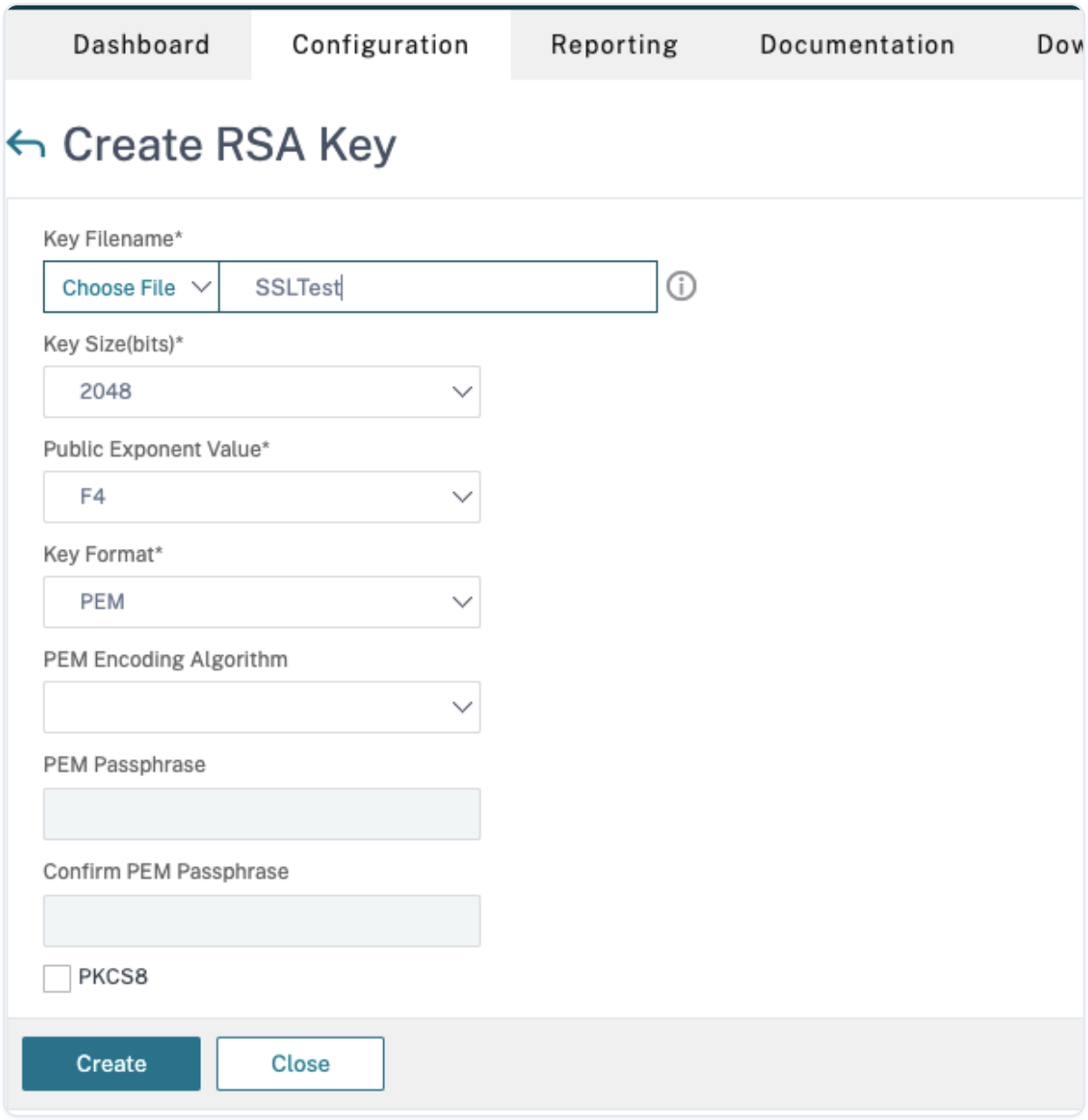
1. Certifique-se de que a seguinte configuração de pré-requisito já esteja em vigor:
   - Os seguintes endereços IP relacionados ao Citrix ADC estão configurados.
     - Endereço IP de Gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



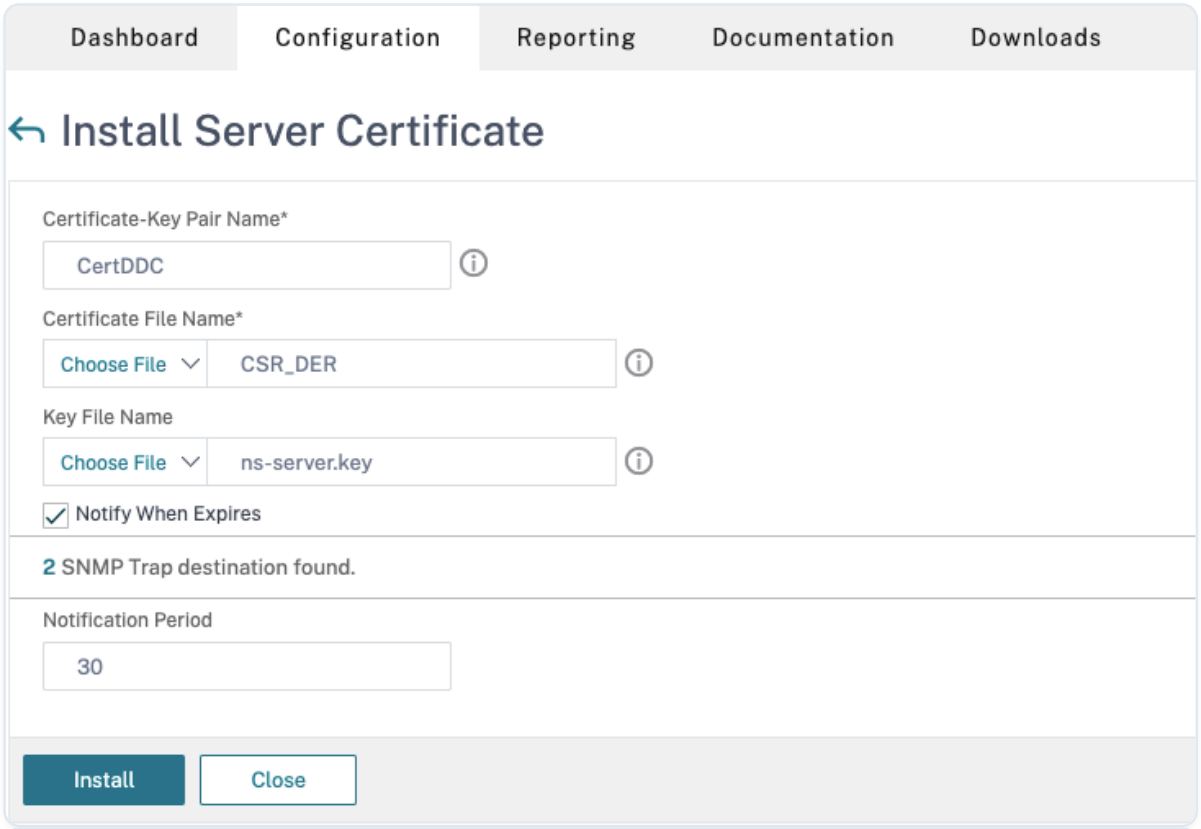
     - Endereço IP de sub-rede (SNIP) para habilitar a comunicação entre o dispositivo Citrix ADC e os servidores de back-end. Para obter detalhes, consulte Configuring Subnet IP Addresses.
     - Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no dispositivo ADC para o lançamento da sessão. Para obter detalhes, consulte Create a virtual server.

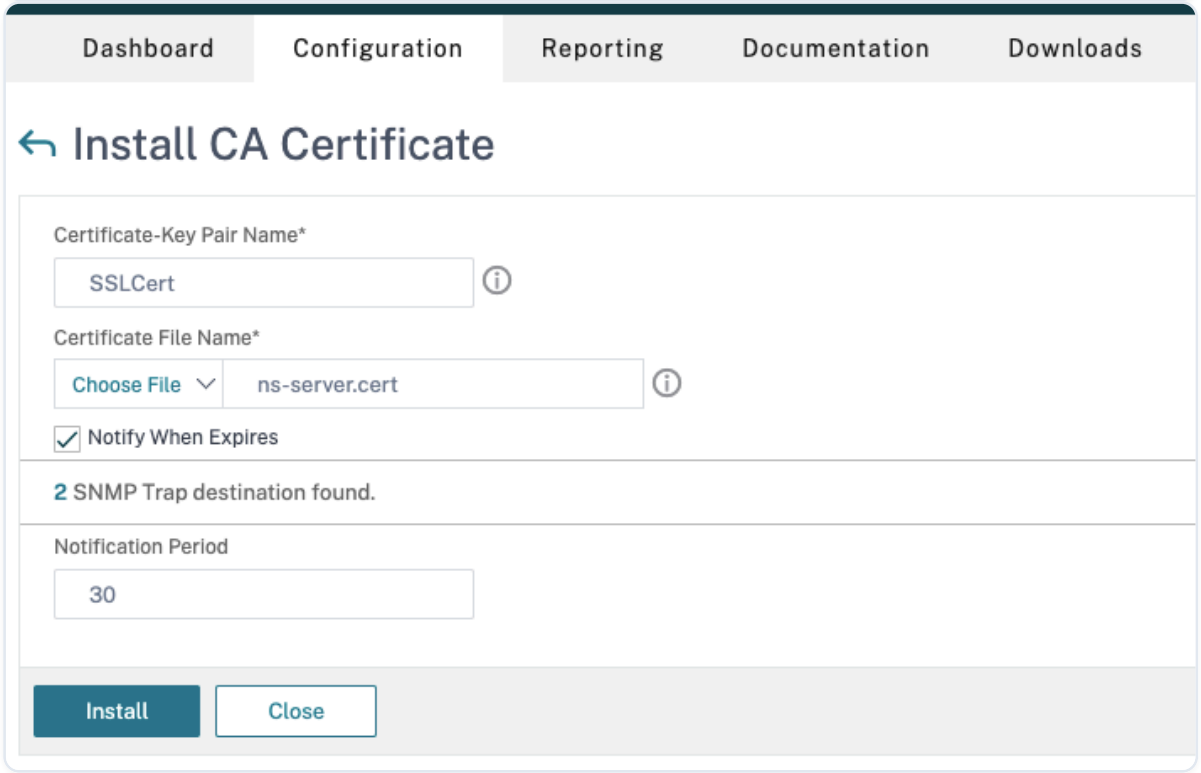


- Os modos e recursos necessários no dispositivo Citrix ADC estão habilitados.
  - Para habilitar os modos, na GUI do Citrix ADC, vá para **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, vá para **System > Settings > Configure Basic Features**.
- As configurações relacionadas a certificados estão concluídas.
  - A Solicitação de Assinatura de Certificado (CSR) é criada. Para obter detalhes, consulte Create a certificate.

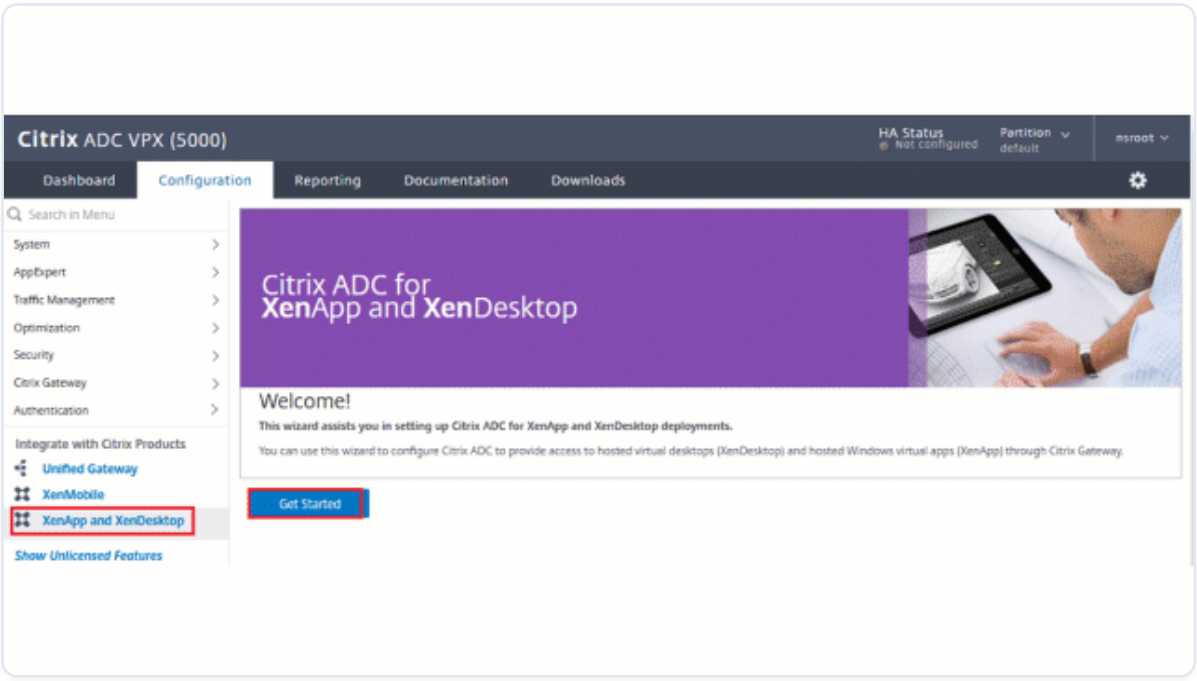


- Os certificados de servidor e CA e os certificados raiz são instalados. Para obter detalhes, consulte Install, link, and updates.





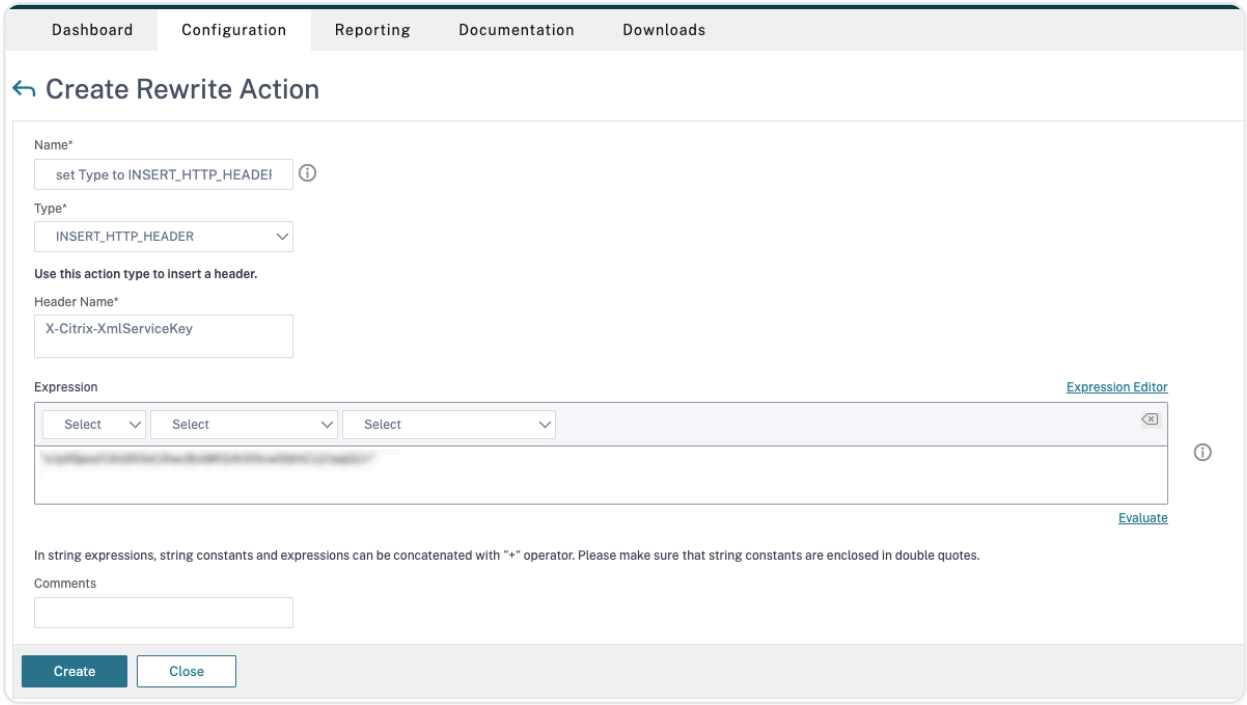
- Um Citrix Gateway foi criado para o Citrix Virtual Desktops. Teste a conectividade clicando no botão **Test STA Connectivity** para confirmar que os servidores virtuais estão online. Para obter detalhes, consulte Configurando o Citrix ADC para Citrix Virtual Apps and Desktops.



2. Adicione uma ação de reescrita. Para obter detalhes, consulte Configuring a Rewrite Action.

   a. Vá para **AppExpert > Rewrite > Actions**.

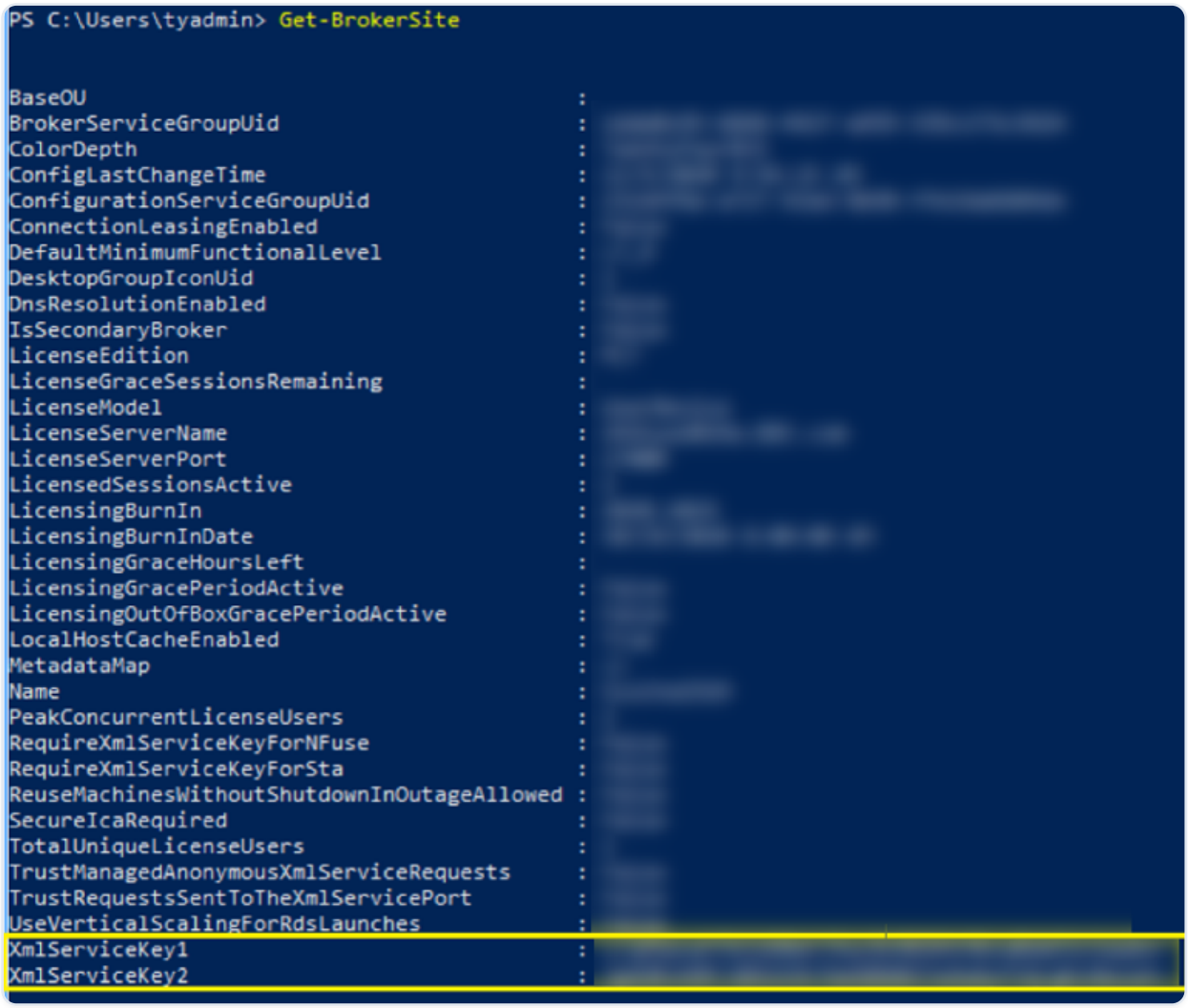
   b. Clique em **Add** para adicionar uma ação de reescrita. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".



   a. Em **Tipo**, selecione **INSERT_HTTP_HEADER**.

   b. Em **Nome do Cabeçalho**, insira X-Citrix-XmlServiceKey.

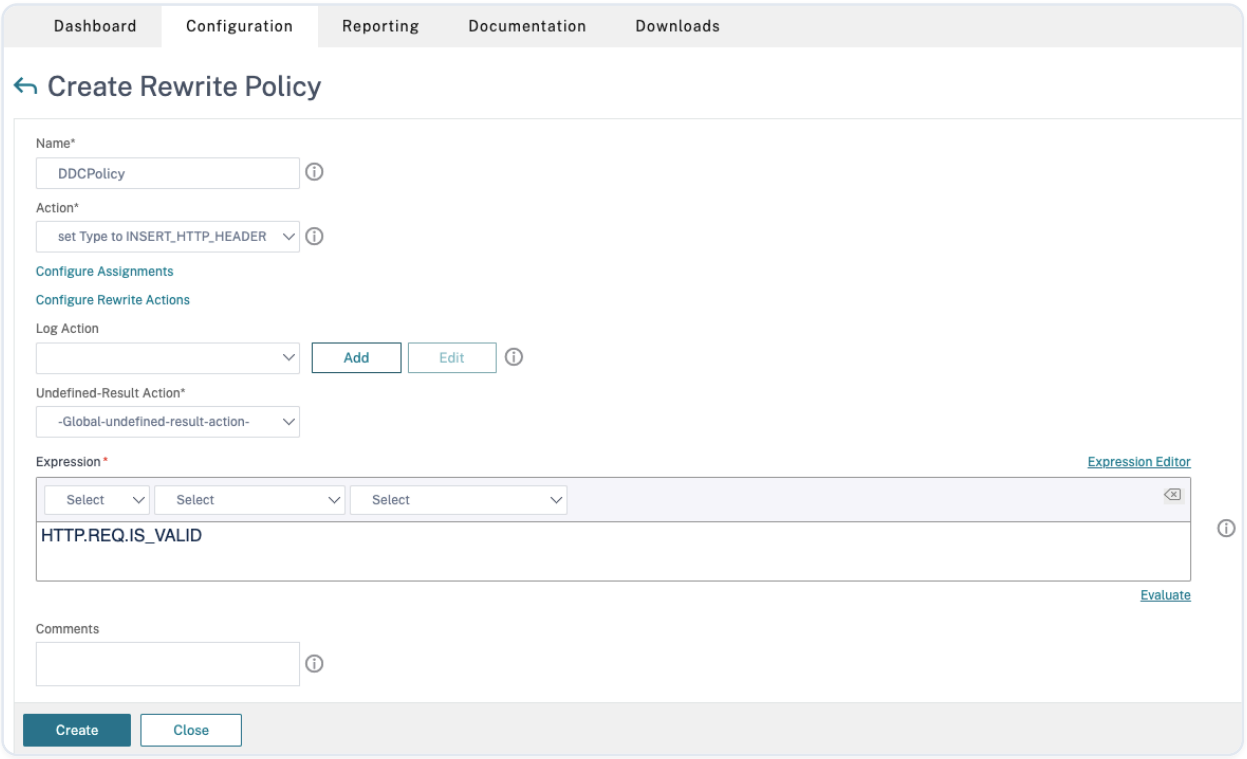
   c. Em **Expressão**, adicione `<XmlServiceKey1 value>` com as aspas. Você pode copiar o valor XmlServiceKey1 da sua configuração do Desktop Delivery Controller™.



3. Adicione uma política de reescrita. Para obter detalhes, consulte Configurando uma Política de Reescrita.

   a. Vá para **AppExpert > Rewrite > Policies**.

   b. Clique em **Add** para adicionar uma política.



a. Em **Ação**, selecione a ação criada na etapa anterior.

b. Em **Expressão**, adicione HTTP.REQ.IS_VALID.

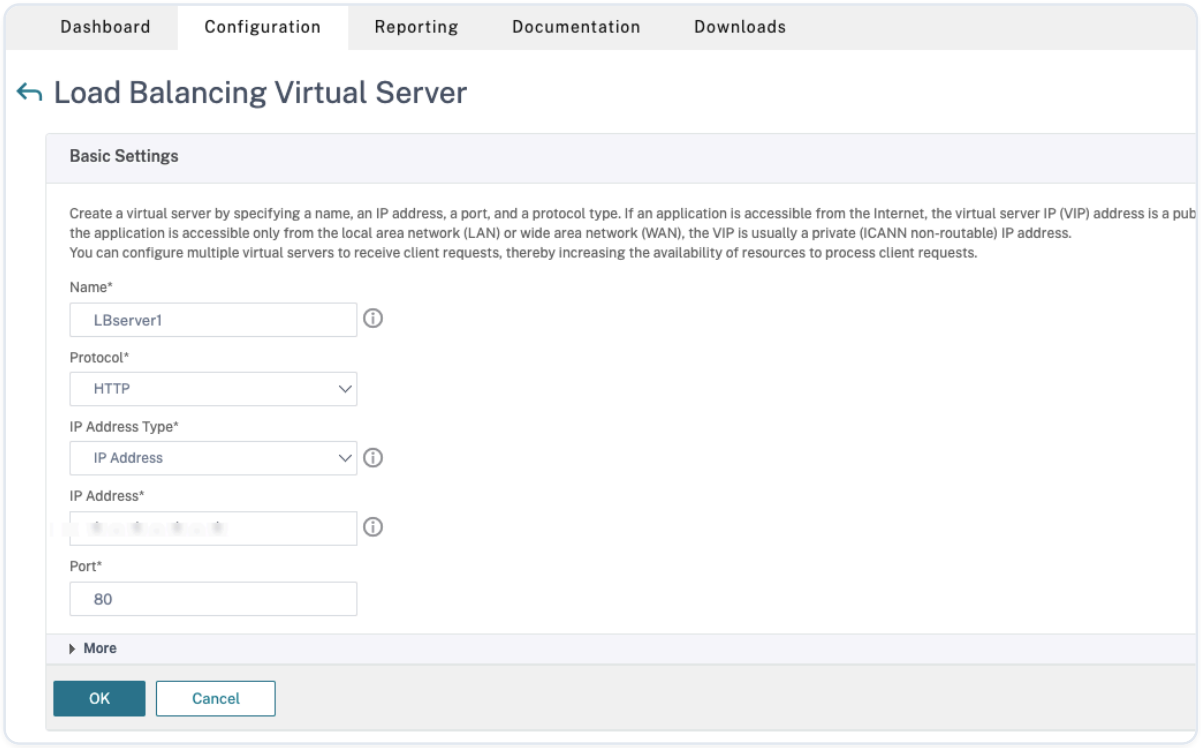
c. Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões não serão iniciadas.

   Para obter detalhes, consulte Configurar balanceamento de carga básico.

   a. Crie um servidor virtual de balanceamento de carga.

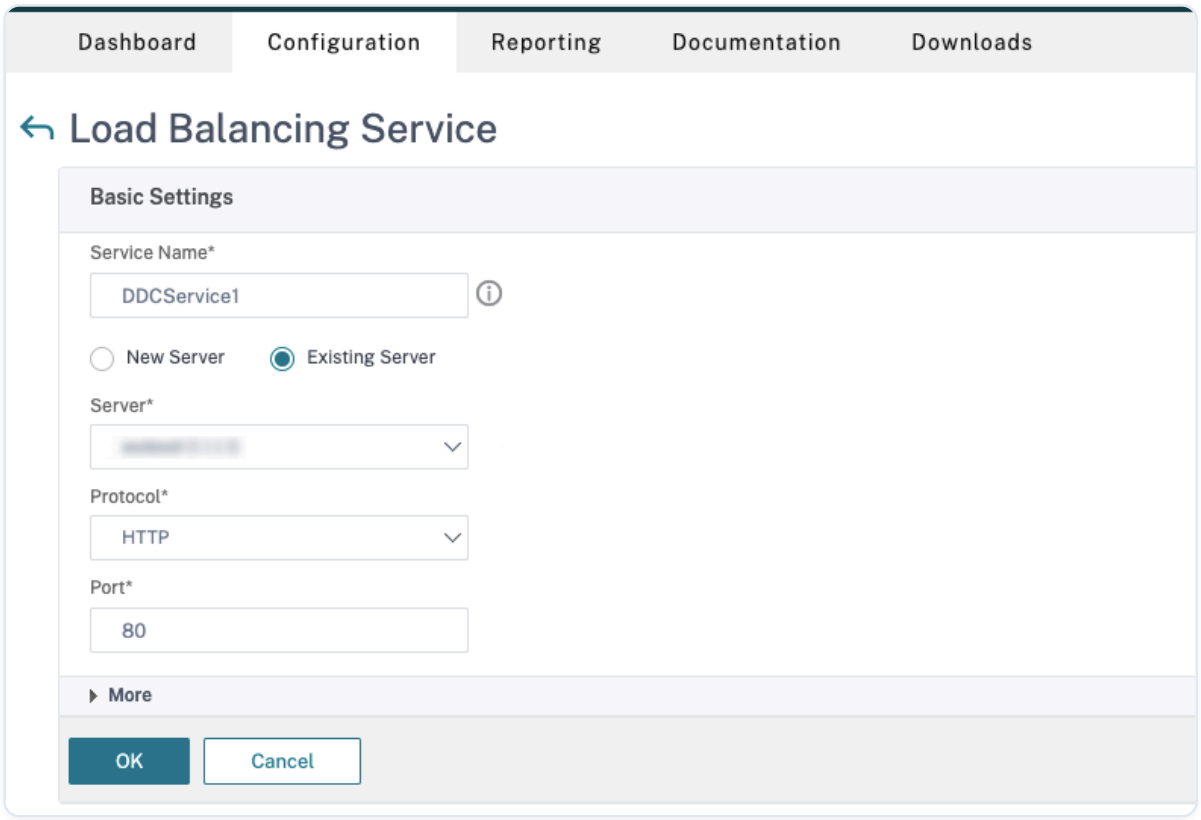
      - Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**.
      - Na página **Virtual Servers**, clique em **Add**.



- 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.

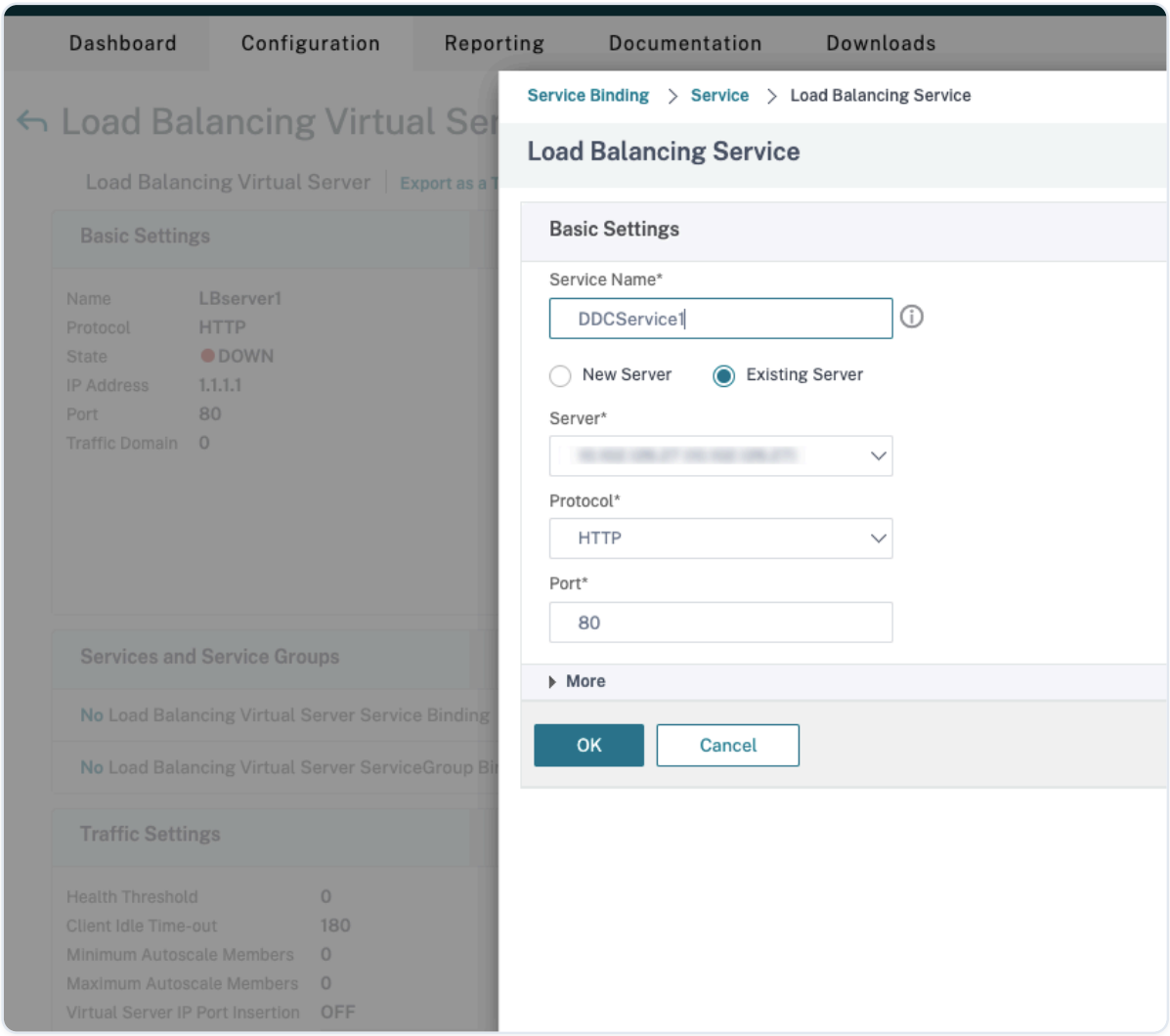
- Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Serviços**.



- 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**.

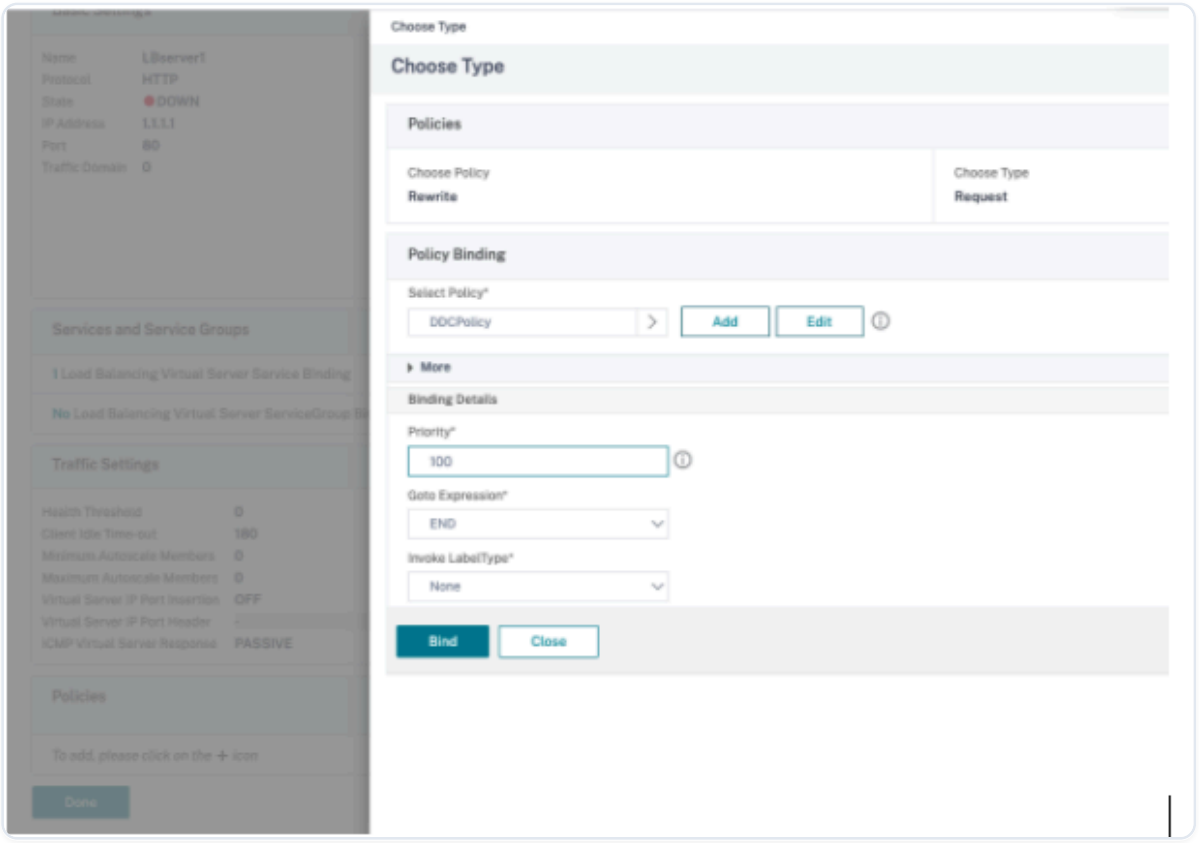


- Em **Service Binding**, selecione o serviço criado anteriormente.
- Clique em **Vincular**.

d. Vincule a política de reescrita criada anteriormente ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.

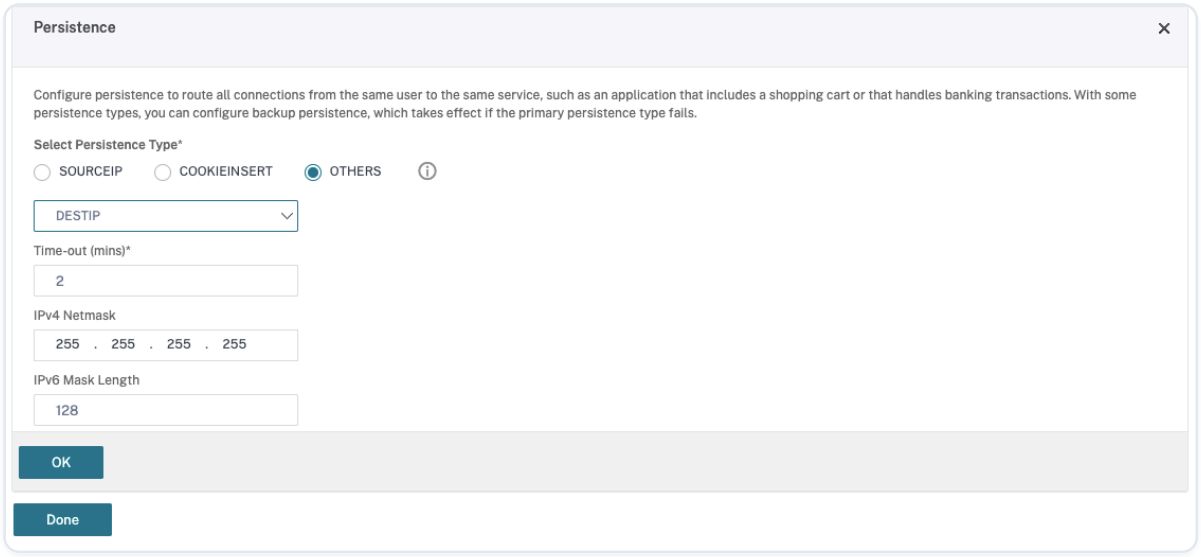
- Em **Configurações Avançadas**, clique em **Políticas,** e, em seguida, na seção **Políticas**, clique em **+**.



- 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**.

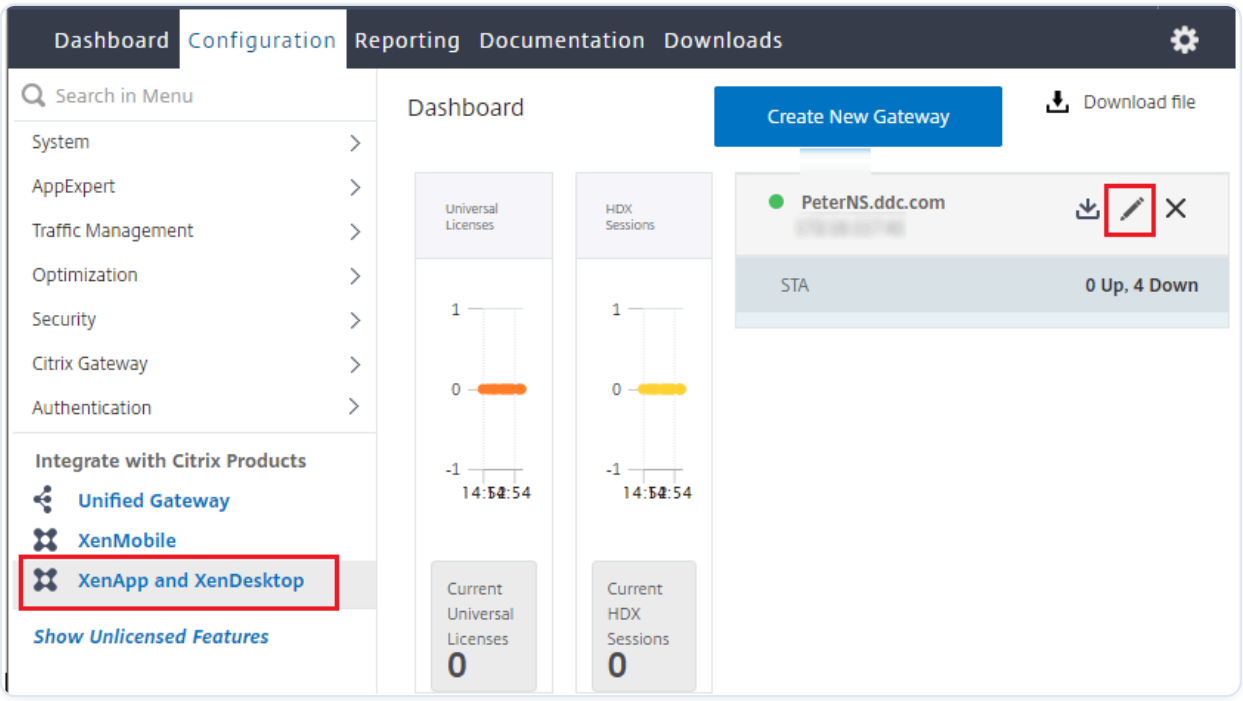
f. Repita estas etapas para o outro servidor virtual também.

Alterações de configuração se o dispositivo Citrix ADC já estiver configurado com Citrix Virtual Desktops™

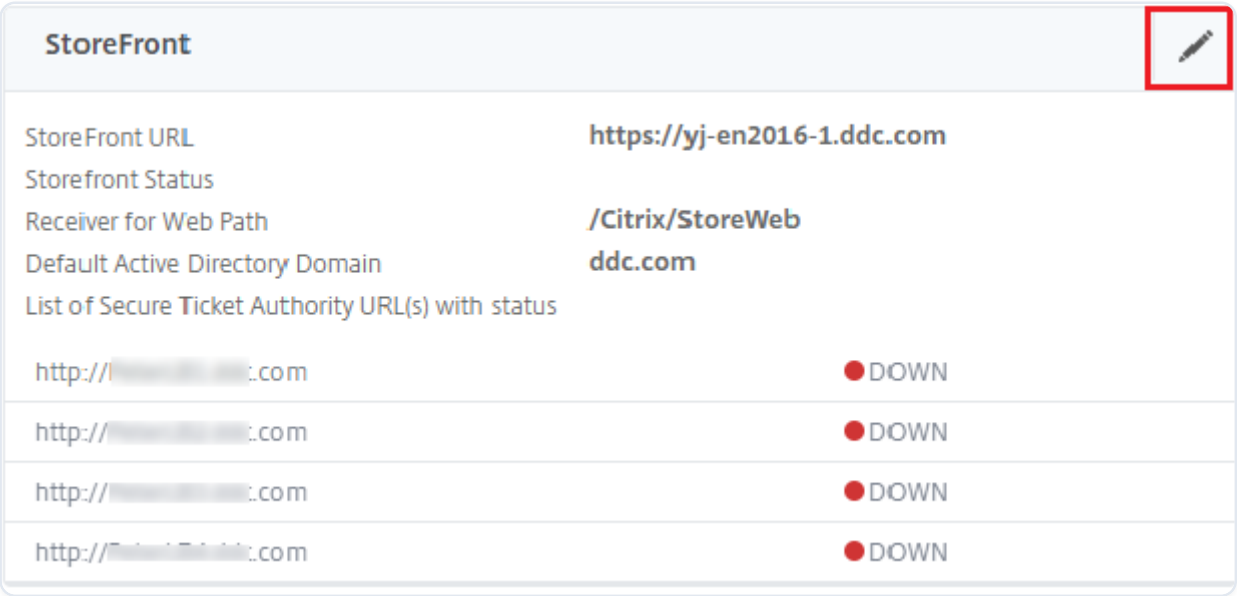
Se você já configurou o dispositivo Citrix ADC com Citrix Virtual Desktops, para usar o recurso Secure XML, você deve fazer as seguintes alterações de configuração.

- 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 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.

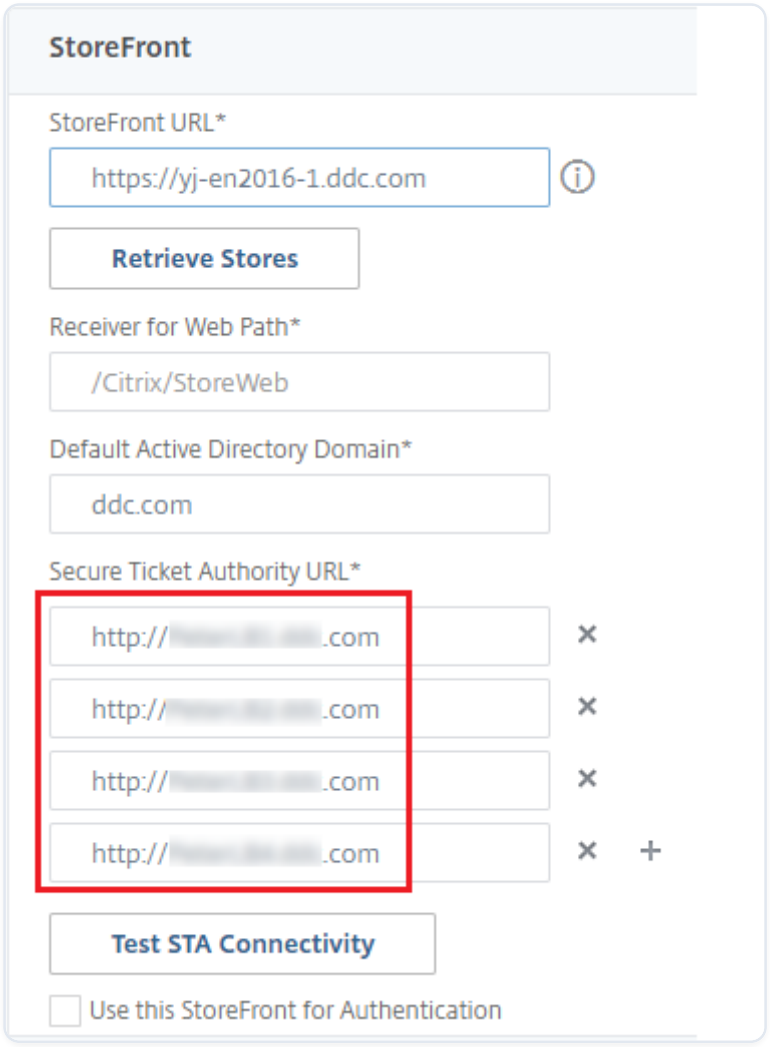


3. No painel StoreFront, clique no ícone de edição.



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.



Sessões

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência ao usuário. Perder a conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode levar à frustração do usuário. Mover-se rapidamente entre dispositivos e acessar os mesmos aplicativos a cada logon é uma prioridade para muitos trabalhadores móveis, como profissionais de saúde.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões, reduzem inconvenientes, tempo de inatividade e perda de produtividade; usando esses recursos, os usuários móveis podem alternar rápida e facilmente entre dispositivos.

Você também pode desconectar um usuário de uma sessão, desconectar uma sessão e configurar o pré-lançamento e a permanência da sessão; consulte Gerenciar grupos de entrega.

Confiabilidade da sessão

A Confiabilidade da Sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Este recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel ferroviário e perde momentaneamente a conectividade. Normalmente, a sessão é desconectada e desaparece da tela do usuário, e o usuário precisa se reconectar à sessão desconectada. Com a Confiabilidade da Sessão, a sessão permanece ativa na máquina. Para indicar a perda de conectividade, a tela do usuário congela e o cursor muda para uma ampulheta giratória até que a conectividade seja retomada do outro lado do túnel. O usuário continua a acessar a exibição 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, este recurso foi projetado para a conveniência do usuário. Portanto, ele não solicita ao usuário uma reautenticação. 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 de porta de confiabilidade da sessão.
- Para evitar que os usuários se reconectem a sessões interrompidas sem precisar se reautenticar, use o recurso Reconexão Automática do Cliente. Você pode configurar a configuração de política de autenticação de Reconexão Automática do Cliente para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usar a Confiabilidade da Sessão e 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 política de tempo limite de confiabilidade da sessão. Depois disso, as configurações de política de Reconexão Automática do Cliente 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 esse recurso está habilitado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Para sessões de aplicativos, 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, esse período é de cinco minutos. Para alterar esse período, edite a seguinte configuração de registro no dispositivo do usuário (onde `seconds` é o número de segundos após os quais 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.

O Auto Client Reconnect incorpora um mecanismo de autenticação baseado em credenciais de usuário criptografadas. Quando um usuário faz logon inicialmente, o servidor criptografa e

armazena as credenciais do usuário na memória. 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 de Auto Client Reconnect. Em vez disso, uma caixa de diálogo é apresentada aos usuários solicitando credenciais quando o Citrix Workspace app tenta se reconectar automaticamente.

Para máxima proteção das credenciais e sessões do usuário, use criptografia para toda a comunicação entre os 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 de conexão também afetam o Auto Client Reconnect:

- Por padrão, o Auto Client Reconnect é habilitado por meio de configurações de política no nível do site, conforme descrito anteriormente. A reautenticação do usuário não é necessária. No entanto, se a conexão ICA TCP de um servidor estiver configurada para redefinir sessões com um link de comunicação interrompido, a reconexão automática não ocorrerá. O Auto Client Reconnect funciona apenas se o servidor desconectar as sessões quando houver uma conexão interrompida ou com tempo limite. Nesse contexto, a conexão ICA TCP refere-se a uma porta virtual de um servidor (em vez de uma conexão de rede real) que é usada para sessões em redes TCP/IP.
- Por padrão, a conexão ICA TCP em um servidor é configurada para desconectar sessões com conexões interrompidas ou com tempo limite. As sessões desconectadas permanecem intactas na memória do sistema e estão disponíveis para reconexão pelo Citrix Workspace app.
- A conexão pode ser configurada para redefinir ou desconectar sessões com conexões interrompidas ou com tempo limite. Quando uma sessão é redefinida, a tentativa de reconexão inicia uma nova sessão. Em vez de restaurar o usuário para o mesmo ponto no aplicativo em uso, o aplicativo é reiniciado.
- Se o servidor estiver configurado para redefinir sessões, o Auto Client Reconnect cria uma nova sessão. Esse processo exige que os usuários insiram suas credenciais para fazer logon no servidor.

- A reconexão automática pode falhar se o Citrix Workspace app ou o plug-in enviar informações de autenticação incorretas, o que pode ocorrer durante um ataque ou se o servidor determinar que muito tempo se passou desde que detectou a conexão interrompida.

ICA Keep-Alive

A habilitação do recurso ICA Keep-Alive impede que conexões interrompidas sejam desconectadas. Quando habilitado, se o servidor não detectar atividade, esse recurso impede que os Serviços de Área de Trabalho Remota desconectem essa sessão. Exemplos de inatividade 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 interrompidas 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 interrompidas 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 ter que reiniciar os desktops ou aplicativos em cada dispositivo. Por exemplo, o controle de workspace pode auxiliar profissionais de saúde em um hospital que precisam se mover rapidamente entre diferentes estações de trabalho e acessar o mesmo conjunto de aplicativos cada vez que fazem logon. Se você configurar as opções de controle de workspace para permitir, esses trabalhadores podem se desconectar de vários aplicativos em um dispositivo cliente e, em seguida, reconectar-se para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle de workspace afeta as seguintes atividades:

- **Fazer logon:** Por padrão, o controle de workspace permite que os usuários se reconectem automaticamente a todos os desktops e aplicativos em execução ao fazer logon, ignorando a necessidade de reabri-los manualmente. Através do controle de workspace, os usuários podem abrir desktops ou aplicativos desconectados, além de quaisquer outros 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.
- **Encerrando sessão:** Para usuários que abrem desktops ou aplicativos através do StoreFront™, você pode configurar o comando **Log Off** para desconectar o usuário do StoreFront e de todas as sessões ativas, ou apenas do StoreFront.
- **Desconectando:** Os usuários podem se desconectar de todos os desktops e aplicativos em execução de uma só vez, sem precisar se desconectar de cada um individualmente.

O controle de espaço de trabalho está disponível apenas para usuários do aplicativo Citrix Workspace que acessam desktops e aplicativos através 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 encerra a sessão de um dispositivo na sala de emergência e, em seguida, faz login 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

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 as sessões atuais existem. 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 de pacientes 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, 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 habilitado, 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 próximos a esse local.
- Quando o roaming de sessão está desabilitado, quando ele faz login em uma máquina diferente (usando as mesmas credenciais), uma nova sessão é iniciada, e impressoras e recursos próximos estarão disponíveis.

Configurar o roaming de sessão

Para configurar o roaming de sessão, use os seguintes cmdlets de regra de política de direito com a propriedade "SessionReconnection". Opcionalmente, você também pode especificar a propriedade "LeasingBehavior".

Para sessões de desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões de aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Sempre:** As sessões sempre fazem roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.
- **SomenteDesconectado:** Reconecte-se apenas a sessões que já estão desconectadas; caso contrário, inicie uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente desconectando-as primeiro ou usando o 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.

- **SomenteMesmoPontoFinal:** Um usuário obtém uma sessão exclusiva para cada dispositivo cliente que usa. Isso desabilita 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 poderá alocar mais tempo para o processo. O padrão para as versões 7.6 e posteriores é de 180 segundos (o padrão para 7.0-7.5 é de 90 segundos).

Na máquina (ou na imagem mestre usada em um catálogo de máquinas), defina a seguinte chave de registro:

Chave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique um tempo decimal em segundos, no intervalo de 0 a 3600.

Se você alterar uma imagem mestre, atualize o catálogo.

Essa configuração se aplica apenas a VMs com VDAs de desktop. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor.

Usar Pesquisa no Studio

Use o recurso de Pesquisa para visualizar informações sobre máquinas específicas, sessões, catálogos de máquinas, aplicativos ou Delivery Groups.

1. Selecione **Pesquisar** no painel de navegação do Studio.

Não é possível pesquisar nas guias de catálogos de máquinas ou Delivery Groups usando a caixa de Pesquisa. Use o nó Pesquisar no painel de navegação.

Para exibir critérios de pesquisa adicionais na exibição, clique no sinal de mais ao lado dos campos suspensos de Pesquisa. Remova os critérios de pesquisa clicando no botão de menos.

2. Insira o nome ou use a lista suspensa para selecionar outra opção de pesquisa para o item que você deseja encontrar.
3. Opcionalmente, salve sua pesquisa selecionando **Salvar como**. A pesquisa aparece na lista **Pesquisas salvas**.

Alternativamente, clique no ícone **Expandir Pesquisa** (dois colchetes angulares para baixo) para exibir um menu de propriedades de pesquisa. Você pode realizar uma pesquisa avançada construindo uma expressão a partir das propriedades no menu.

Dicas para aprimorar uma pesquisa:

- Para exibir características adicionais para incluir na exibição na qual você pode pesquisar e classificar, clique com o botão direito em qualquer coluna e selecione **Selecionar colunas**.
- 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 Delivery Group, selecione **Delivery Groups** no painel de navegação, em seguida, selecione o grupo e, em seguida, selecione **Exibir Máquinas** no painel Ações.

Tags

Introdução

As tags são cadeias de caracteres 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 Studio.

Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma tag chamada “test” e adicione-a (aplique-a) a esses aplicativos. Agora você pode filtrar a pesquisa do 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 reinicializações periódicas 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 reinicialização para subconjuntos de máquinas em um grupo de entrega. Para exemplos e detalhes, consulte Gerenciar grupos de entrega.

- Adaptar a aplicação (atribuição) de políticas Citrix® a um subconjunto de máquinas em grupos de entrega, tipos de grupo de entrega ou UOs que tenham (ou não tenham) uma tag especificada.

  Por exemplo, se você quiser aplicar uma política Citrix apenas às estações de trabalho mais poderosas, 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 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

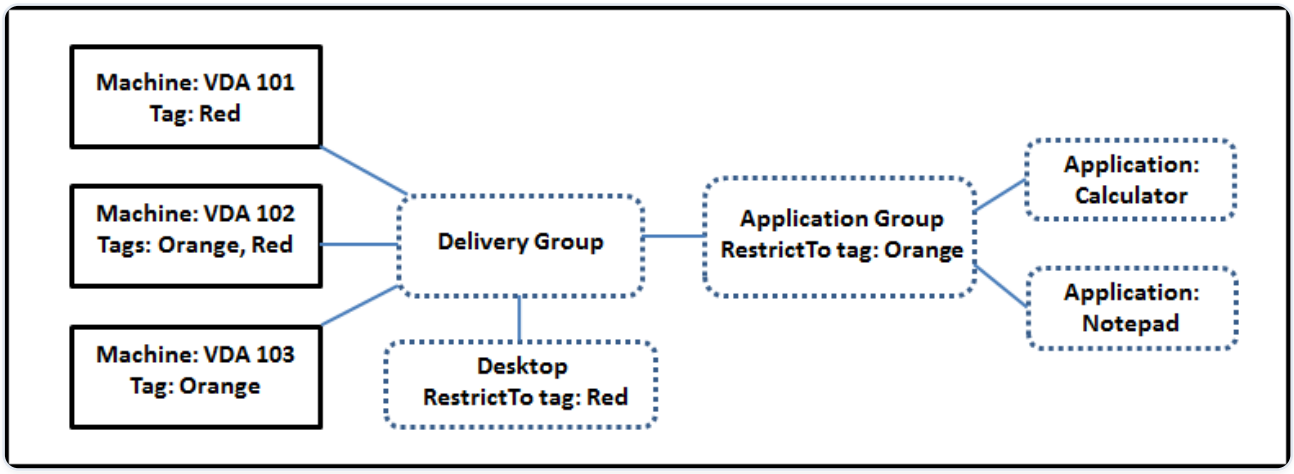
Uma restrição de tag envolve várias etapas:

- 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.



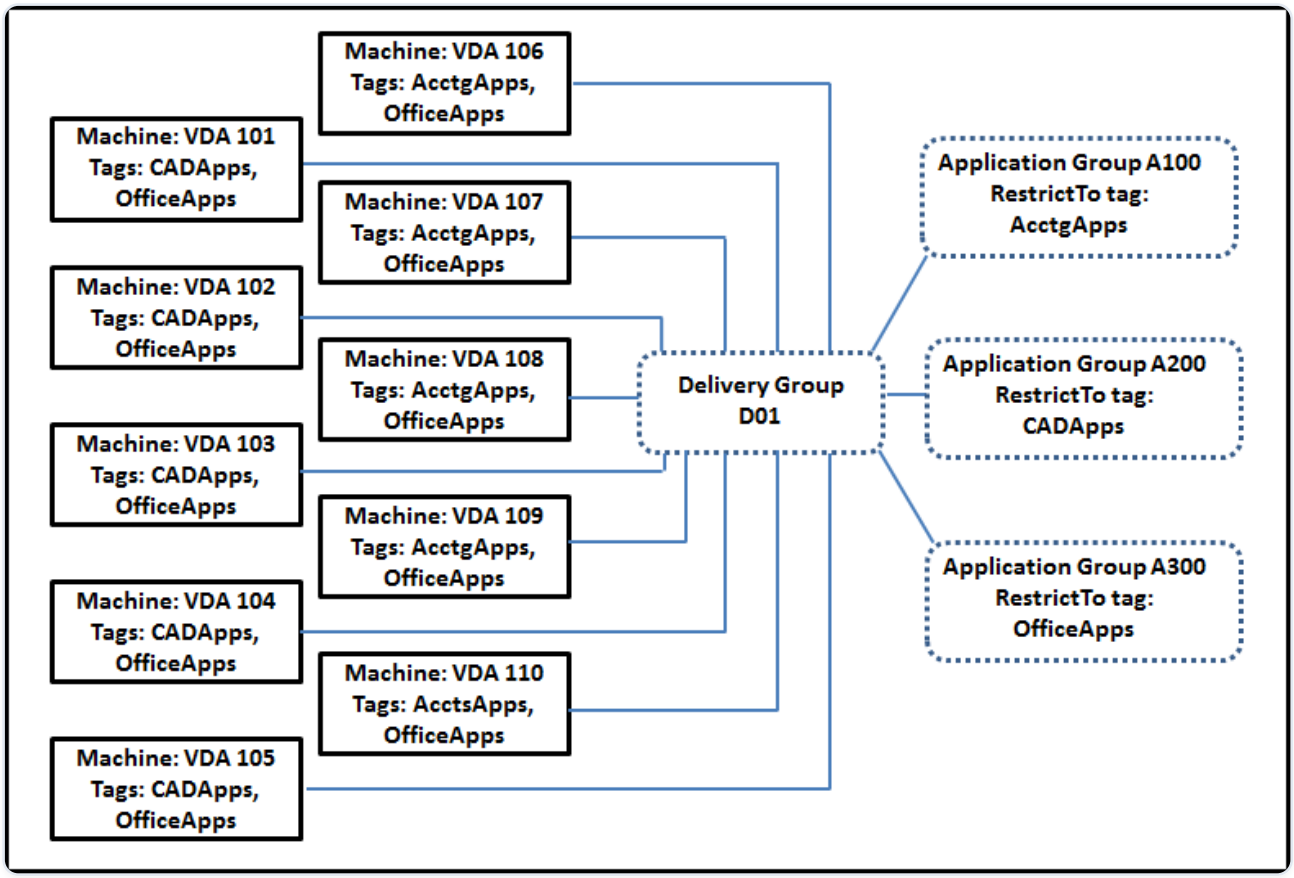
- Tags foram adicionadas a cada uma das três máquinas (VDA 101-103).
- O desktop no grupo de entrega compartilhado foi criado com uma restrição de tag chamada "Red". Um desktop pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Red": VDA 101 e 102.
- O grupo de aplicativos 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 possui ambas as tags (Red e Orange), portanto, 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 de 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 Studio.

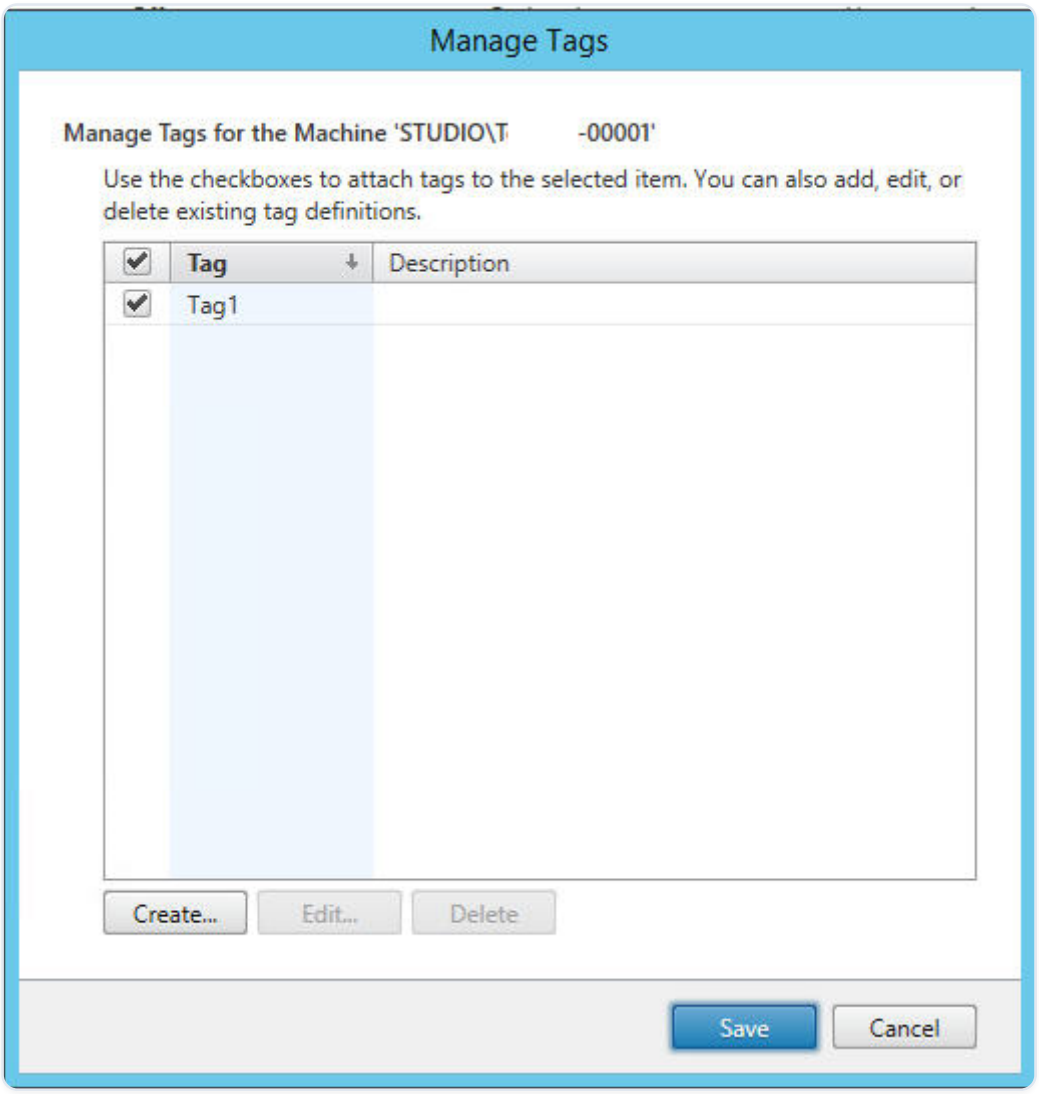
(Exceção: As tags usadas para atribuições de política são criadas, editadas e excluídas por meio da ação **Gerenciar Tags** no Studio. No entanto, as tags são aplicadas (atribuídas) quando você cria a política. Consulte Criar políticas para obter detalhes.)

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 Studio

No 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** no painel 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 na disponibilização dessas máquinas 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 Studio para excluir uma tag que é usada como restrição. Primeiro, edite o grupo de aplicativos e remova a restrição da tag ou selecione uma tag diferente.

Quando terminar na caixa de diálogo Gerenciar Tags, clique em **Salvar**.

Para ver se uma máquina tem alguma tag aplicada: Selecione **Grupos de Entrega** no painel de navegação. Selecione um grupo de entrega no painel central e, em seguida, selecione **Exibir Máquinas** no painel Ações. Selecione uma máquina no painel central e, em seguida, selecione a guia **Tags** no painel **Detalhes**.

Gerenciar restrições de tags

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 **Delivery Groups**, 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 **Delivery Groups**, selecione uma tag diferente na lista ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

- **Para adicionar uma restrição de tag a uma área de trabalho:**

  Crie ou edite um grupo de entrega. Clique em **Adicionar** ou **Editar** na página **Desktops**. 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 Desktops, clique em **Editar**. Na caixa de diálogo, selecione uma tag diferente nas 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 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 o lançamento de aplicativos ou áreas de trabalho adicionais. Se for 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 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 Studio avisa que você não pode excluir a tag até editar o grupo para removê-la como uma restrição. (Se você tivesse permissão para excluir uma tag que é usada como restrição em um grupo de aplicativos, isso poderia resultar em permitir que os aplicativos fossem iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição de exclusão de uma tag se aplica se a tag estiver sendo usada como restrição para inicializações de desktop. Depois de editar o grupo de aplicativos ou desktops no grupo de entrega para remover essa restrição de tag, você pode excluir a tag.

Nem todas as máquinas podem ter os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada um com uma restrição de tag diferente e conjuntos de máquinas diferentes ou sobrepostos de grupos de entrega. A tabela a seguir lista como as considerações da máquina são decididas.

QUANDO UM APLICATIVO FOI ADICIONADO A	ESTAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO
Um grupo de aplicativos sem restrição de tag	Qualquer máquina.
Um grupo de aplicativos com restrição de tag A	Máquinas que têm a tag A aplicada.
Dois grupos de aplicativos, um com restrição de tag A e o outro com restrição de tag B	Máquinas que têm a tag A e a tag B. Se nenhuma estiver disponível, então máquinas que têm a tag A ou a tag B.
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 faça 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 Studio, selecione o grupo de entrega D01 e, em seguida, selecione **View Machines** no painel Ações.
2. Selecione as máquinas VDA 101-105 e, em seguida, selecione **Manage Tags** no painel Ações.
3. Na caixa de diálogo Manage Tags, clique em **Create** e, em seguida, crie uma tag chamada `CADApps`. Clique em **OK**.
4. Clique em **Create** novamente e crie uma tag chamada OfficeApps. Clique em **OK**.
5. Ainda na caixa de diálogo **Manage 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 **View Machines** no painel Ações.
7. Selecione as máquinas VDA 106-110 e, em seguida, selecione **Manage Tags** no painel Ações.
8. Na caixa de diálogo **Manage Tags**, clique em **Create**. Crie uma tag chamada `AcctgApps`. Clique em **OK**.
9. Aplique a tag `AcctgApps` recém-criada e a tag `OfficeApps` às máquinas selecionadas, marcando as caixas de seleção ao lado do nome de cada tag e, em seguida, feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de tag.

1. No Studio, selecione **Applications** no painel de navegação e, em seguida, selecione **Create Application Group** no painel Ações. O assistente Create Application Group é iniciado.
2. Na página **Delivery Groups** do assistente, selecione o grupo de entrega D01. Selecione **Restrict launches to machines with tag** e, em seguida, selecione a tag `AcctgApps` na lista.
3. Complete o assistente, especificando os usuários contábeis e os aplicativos contábeis. (Ao adicionar o aplicativo, escolha a fonte **Do menu Iniciar**, que pesquisa o aplicativo nas máquinas que têm a tag `AcctgApps`.) Na página **Resumo**, nomeie o grupo `A100`.
4. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando as máquinas que têm a tag `CADApps`, além dos usuários e aplicativos apropriados.

5. Repita as etapas para criar o grupo de aplicativos `A300`, especificando as máquinas que têm a tag `OfficeApps`, além dos usuários e aplicativos apropriados.

Tags em catálogos de máquinas

Você pode usar tags em catálogos de máquinas. A sequência geral de criação de uma tag e sua aplicação a um catálogo é a mesma descrita anteriormente. No entanto, a aplicação de tags a catálogos é suportada apenas por meio da interface do PowerShell. Você não pode usar o Studio para aplicar uma tag a um catálogo ou remover uma tag de um catálogo. As exibições de catálogo no Studio não indicam se uma tag foi aplicada.

Resumo: Você pode usar o 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 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 Studio ou o PowerShell.)

Consulte a ajuda do cmdlet do PowerShell para obter mais orientações e sintaxe.

Mais informações

Postagem de blog: Como atribuir desktops a servidores específicos.

Suporte a IPv4/IPv6

Esta versão oferece suporte a implantações puras de IPv4, puras de IPv6 e dual-stack que usam redes IPv4 e IPv6 sobrepostas.

Os componentes a seguir suportam apenas IPv4. Todos os outros suportam IPv4 e IPv6.

- Citrix Provisioning™
- Citrix Hypervisor™
- Virtual Delivery Agents (VDAs) não controlados pela configuração de política **Only use IPv6 Controller registration**

As comunicações IPv6 são controladas por duas configurações de política Citrix® relacionadas à conexão do 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 com o 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.

Esta configuração é válida apenas quando a configuração **Only use IPv6 Controller registration policy** estiver ativada. Padrão = String vazia

Considerações sobre a implantação

Se seu ambiente contiver redes IPv4 e IPv6, crie configurações de grupo de entrega separadas para clientes somente IPv4 e para os clientes que podem acessar a rede IPv6. Considere usar nomenclatura, atribuição manual de grupo do Active Directory ou filtros SmartAccess para diferenciar usuários.

A reconexão da sessão pode falhar se a conexão for iniciada em uma rede IPv6, e você tentar se conectar novamente de um cliente que tem apenas acesso IPv4.

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 necessidades variadas dos seus usuários, você pode usar as políticas do Citrix Virtual Apps and Desktops™ para aplicar comportamentos de perfil diferentes às máquinas em cada Delivery Group. Por exemplo, um Delivery Group pode exigir perfis obrigatórios do Citrix, cujo modelo é armazenado em um local de rede, enquanto outro Delivery Group 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 configurem quaisquer políticas relacionadas a perfis em seus Delivery Groups.
- 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 área de trabalho 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 que persista quando o sistema é desligado. Sistemas persistentes podem empregar tecnologia de armazenamento como SANs para fornecer emulação de disco local. Em contraste, sistemas provisionados são criados "em tempo real" a partir de um disco base e algum tipo de disco de identidade. O armazenamento local é geralmente emulado por um disco RAM ou disco de rede, sendo este último frequentemente fornecido por uma SAN com um link de alta velocidade. A tecnologia de provisionamento é geralmente Citrix Provisioning ou Machine Creation Services™ (ou um equivalente de terceiros). Às vezes, sistemas provisionados possuem armazenamento local persistente. Estes são classificados como persistentes.

Juntos, esses dois fatores definem os seguintes tipos de máquina:

- **Ambos persistentes e dedicados** -- Exemplos são máquinas de SO de sessão única com atribuição estática e armazenamento local persistente que são criadas com Machine Creation Services, desktops com armazenamento persistente que são criados com VDI-in-a-Box, 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

- **Ambos provisionados e dedicados** -- Exemplos são máquinas de SO de sessão única com atribuição estática, mas sem armazenamento persistente, que são criadas com Citrix Provisioning™
- **Ambos provisionados e compartilhados** -- Exemplos são máquinas de SO de sessão única com atribuição aleatória que são criadas com Citrix Provisioning e desktops sem armazenamento persistente que são criados com VDI-in-a-Box

As seguintes configurações de política de Gerenciamento de Perfil 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 **Streaming de perfil** está desativado para este tipo de máquina, a configuração **Sempre armazenar em cache** é sempre ignorada.
2. Desative **Sempre armazenar em cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, ativando esta política e usando-a para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo desse tamanho ou maior é armazenado em cache localmente o mais rápido possível.
3. Desative **Gravação ativa** exceto para salvar alterações nos perfis de usuários que alternam entre servidores Citrix Virtual Apps. Neste caso, ative esta política.
4. Desative **Processar logons de administradores locais** exceto para Desktops Compartilhados Hospedados. Neste caso, ative esta política.
5. Desative **Excluir perfis armazenados em cache localmente no 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. Desative **Sempre armazenar em cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, ativando esta política e usando-a para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo desse tamanho ou maior é armazenado em cache localmente o mais rápido possível.
7. Ative **Processar logons de administradores locais** exceto para perfis de usuários que alternam entre servidores Citrix Virtual Apps e Desktops. Neste caso, desative esta política.

Redirecionamento de pasta

O redirecionamento de pasta permite armazenar dados do usuário em compartilhamentos de rede diferentes do local onde os perfis são armazenados. O redirecionamento de pasta reduz o tamanho do perfil e o tempo de carregamento, mas pode impactar a largura de banda da rede. O redirecionamento de pasta não exige que os perfis de usuário do Citrix sejam empregados. Você pode optar por gerenciar seus próprios perfis de usuário e ainda redirecionar pastas.

Configure o redirecionamento de pasta usando políticas Citrix no Studio.

- Certifique-se de que os locais de rede usados para armazenar o conteúdo das pastas redirecionadas estejam disponíveis e tenham as permissões corretas. As propriedades do local são validadas.
- As pastas redirecionadas são configuradas na rede e seu conteúdo é preenchido a partir dos desktops virtuais dos usuários no logon.

Configure o redirecionamento de pasta usando apenas Políticas Citrix ou Objetos de Política de Grupo do Active Directory, não ambos. A configuração do redirecionamento de pasta usando ambos os mecanismos de política pode resultar em comportamento imprevisível.

Redirecionamento avançado de pasta

Em implantações com vários sistemas operacionais (SOs), você pode querer que parte do perfil de um usuário seja compartilhada por cada SO. O restante do perfil não é compartilhado e é usado apenas por um SO. Para garantir uma experiência de usuário consistente entre os SOs, você precisa de uma configuração diferente para cada SO, ou seja, redirecionamento avançado de pasta. Por exemplo, diferentes versões de um aplicativo em execução em dois SOs podem precisar ler ou editar um arquivo compartilhado, então você decide redirecioná-lo para um único local de rede onde ambas as versões possam acessá-lo. Alternativamente, como o conteúdo da pasta **Menu Iniciar** está estruturado de forma diferente em dois SOs, você decide redirecionar apenas uma pasta, não ambas. Essa abordagem separa a pasta **Menu Iniciar** e seu conteúdo em cada SO, garantindo uma experiência consistente para os usuários.

Se sua implantação exigir 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 de Aplicativo	Não	Não
Contatos	Sim	Sim
Área de Trabalho	Sim	Não
Downloads	Não	Não
Favoritos	Sim	Sim

PASTA	REDIRECIONADO NO WINDOWS 10?	REDIRECIONADO NO WINDOWS SERVER 2019?
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 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 originarem de uma máquina Windows 10, mas não de uma máquina Windows Server.
- Para as pastas não redirecionadas:

- Você não quer sobrecarregar seus servidores com arquivos baixados pelos usuários, então você escolhe não redirecionar a pasta Downloads
- Dados de aplicativos individuais podem causar problemas de compatibilidade e desempenho, então você decide não redirecionar a pasta Dados de Aplicativos

Para obter mais informações sobre o redirecionamento de pastas, consulte Visão geral do redirecionamento de pastas, arquivos offline e perfis de usuário móveis.

Redirecionamento de pastas e exclusões

No Citrix Profile Management (mas não no Studio), uma melhoria de desempenho permite que você impeça que pastas sejam processadas usando exclusões. Se você usar esse recurso, não exclua nenhuma pasta redirecionada. Os recursos de redirecionamento de pastas e exclusão funcionam juntos. Garantir que nenhuma pasta redirecionada seja excluída permite que o Profile Management as mova de volta para a estrutura da pasta de perfil e preserve a integridade dos dados se você decidir mais tarde não redirecioná-las. Para obter mais informações sobre exclusões, consulte Incluir e excluir itens.

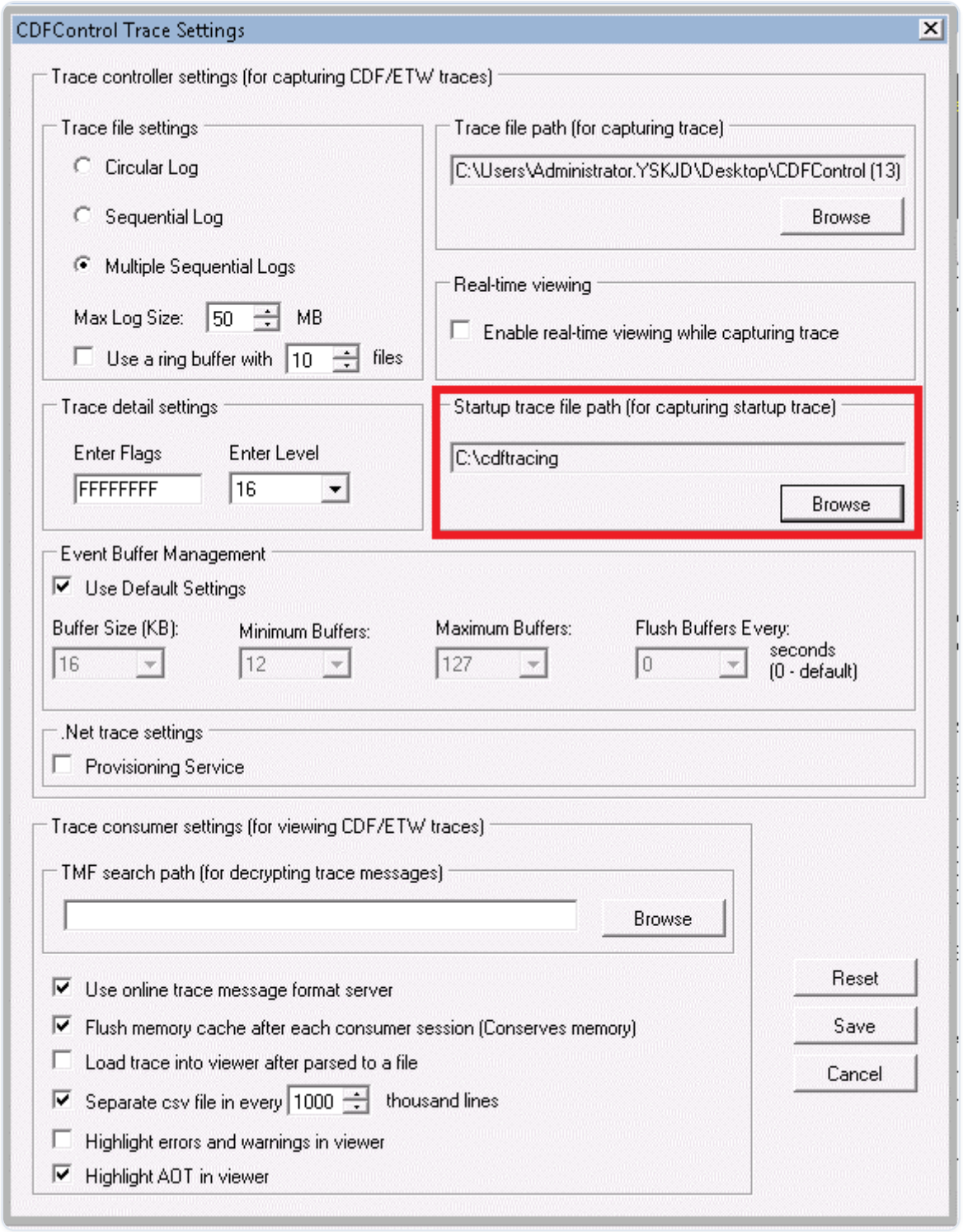
Coletar um rastreamento do Citrix Diagnostic Facility (CDF) na inicialização do sistema

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 se destina a solucionar problemas complexos relacionados ao Citrix, analisar o suporte a filtros e coletar dados de desempenho. Para baixar o utilitário CDFControl, consulte CTX111961.

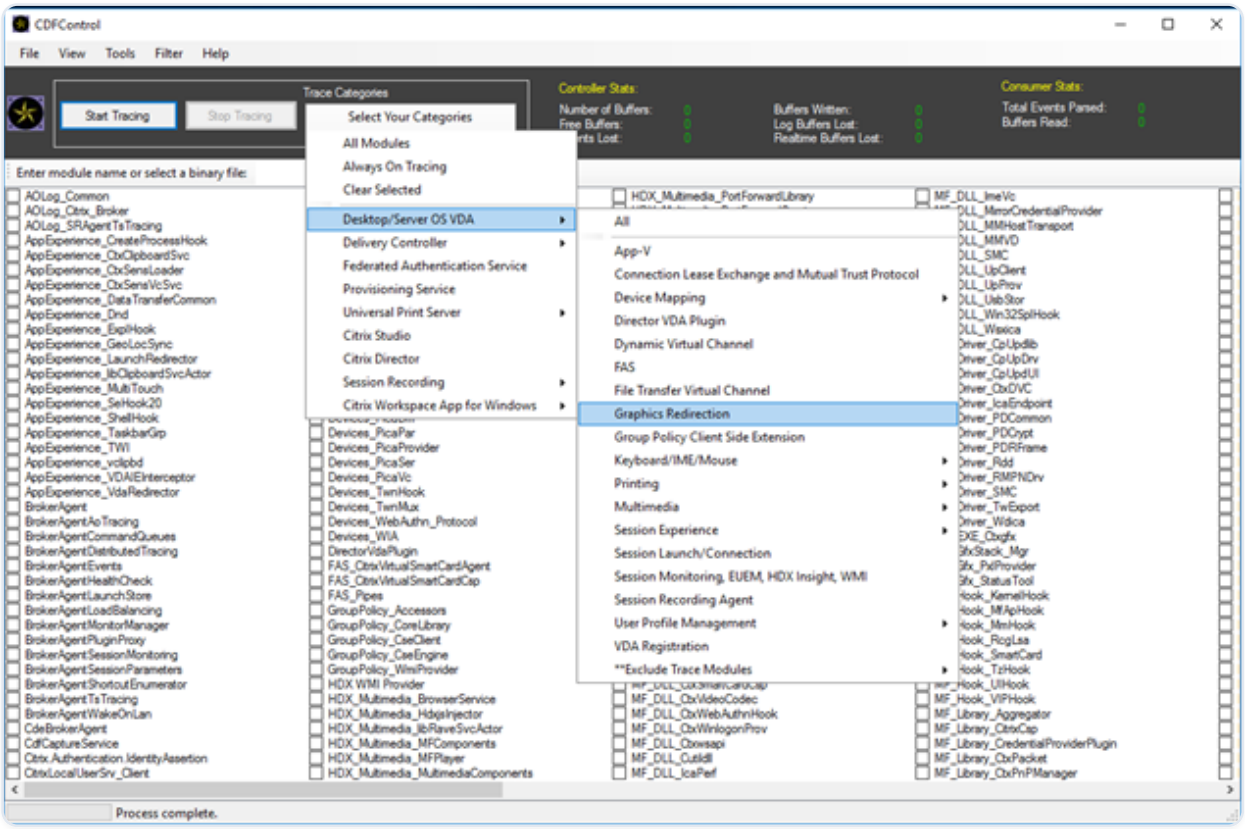
Coletar um rastreamento na inicialização do sistema

Use o procedimento a seguir para coletar um rastreamento CDF na inicialização do sistema. Você precisa de privilégios de administrador.

1. Inicie o **CDFControl** e selecione **Opções** no menu **Ferramentas**.
2. Especifique o caminho do arquivo de rastreamento na seção **Caminho do arquivo de rastreamento de inicialização para capturar rastreamento de inicialização**. Em seguida, clique em **Salvar**.



3. Selecione as **Trace Categories** recomendadas pelo Suporte Citrix. (No exemplo a seguir, **Graphics Redirection** está selecionado. Essa seleção é apenas um exemplo. Recomendamos que você habilite os provedores para o problema específico que está solucionando.)



4. Selecione **Rastreamento de Inicialização** e selecione **Habilitar** no menu **Ferramentas**.

   Após selecionar **Enable**, a barra animada começa a rolar. Essa atividade não afeta o procedimento. Continue para a próxima etapa.

5. Depois que o **Startup Tracing** estiver habilitado, feche o **utilitário CDFControl** e reinicie o sistema.

6. Inicie o utilitário **CDFControl**. Depois que o sistema reiniciar e o erro aparecer, desabilite o rastreamento de inicialização selecionando **Startup Tracing** no menu **Tools** e clicando em **Disable**.

7. Vá para o caminho do arquivo de rastreamento especificado na etapa 2 e colete o arquivo de log de rastreamento (.etl) para análise.

Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios. Suas capacidades de instrumentação e telemetria permitem que usuários técnicos (clientes, parceiros e engenheiros) autodiagnostiquem e corrijam problemas e otimizem seus ambientes. Para detalhes e as informações mais recentes sobre o CIS e como ele funciona, consulte `<https://cis.citrix.com>` (credenciais de conta Citrix necessárias).

Todas as informações carregadas para a Citrix são usadas para fins de solução de problemas e diagnóstico, e para melhorar a qualidade, confiabilidade e desempenho dos produtos, sujeitas a:

- Política de Serviços do Citrix Insight em `<https://cis.citrix.com/legal>`
- Política de Privacidade da Citrix em `<https://www.cloud.com/privacy-policy>`

Esta versão do Citrix Virtual Apps and Desktops™ oferece suporte às seguintes tecnologias.

- Análise de instalação e atualização do Citrix Virtual Apps and Desktops
- Programa de Melhoria da Experiência do Cliente Citrix (CEIP)
- Citrix Call Home
- Citrix Scout

Além (e separadamente) do CIS e do Citrix Analytics: o Google Analytics é coletado (e posteriormente carregado) automaticamente quando você instala (ou atualiza) o Studio. Após instalar o Studio, você pode alterar essa configuração com a chave de registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Um valor de 1 habilita a coleta e o upload, 0 desabilita a coleta e o upload.

Análise de instalação e atualização

Ao usar o instalador completo do produto para implantar ou atualizar componentes do Citrix Virtual Apps and Desktops, informações anônimas sobre o processo de instalação são coletadas e armazenadas na máquina onde você está instalando/atualizando o componente. Esses dados são usados para ajudar a Citrix a melhorar as experiências de instalação de seus clientes.

As informações são armazenadas localmente em `%ProgramData%\Citrix\CTQs`.

O upload automático desses dados é habilitado por padrão nas interfaces gráfica e de linha de comando do instalador completo do produto.

- Você pode alterar o valor padrão em uma configuração de registro. Se você alterar a configuração de registro antes de instalar/atualizar, esse valor será usado quando você usar o instalador completo do produto.
- Você pode substituir a configuração padrão se instalar/atualizar com a interface de linha de comando, especificando uma opção com o comando.

Controlar uploads automáticos:

- Configuração de registro que controla o upload automático de análises de instalação/atualização (padrão = 1):

  - Local: `HKLM:\Software\Citrix\MetaInstall`
  - Nome: SendExperienceMetrics
  - Valor: 0 = 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

Quando você participa do Programa de Melhoria da Experiência do Cliente Citrix (CEIP), estatísticas anônimas e informações de uso são enviadas à Citrix para ajudar a Citrix a melhorar a qualidade e o desempenho dos produtos Citrix. Para obter mais informações, consulte https://more.citrix.com/XD-CEIP.

Inscrição durante a criação ou atualização do Site

Você é automaticamente inscrito no CEIP ao criar um Site (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 **Configuração** no painel de navegação do Studio (guia **Suporte ao Produto**) e siga as orientações.

Ao atualizar uma implantação do Citrix Virtual Apps and Desktops:

- Se você atualizar de uma versão que não suportava o CEIP, será perguntado se deseja participar.
- Se você atualizar de uma versão que suportava o CEIP, e a participação estava ativada, o CEIP é ativado no Site atualizado.
- Se você atualizar de uma versão que suportava o CEIP, e a participação estava desativada, o CEIP é desativado no Site atualizado.

- Se você atualizar de uma versão que suportava o CEIP, e a participação é desconhecida, você 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 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 gravados periodicamente 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 determinados 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, em

seguida, carrega periodicamente pacotes de telemetria contendo esses dados diretamente para o Citrix Insight Services (via HTTPS na porta padrão 443) para análise e solução de problemas.

No Citrix Virtual Apps and Desktops, o Call Home é executado como um serviço em segundo plano sob o nome Citrix Telemetry Service. Para obter mais informações, consulte https://more.citrix.com/XD-CALLHOME.

A funcionalidade de agendamento do Call Home também está disponível no Citrix Scout. Para obter detalhes, consulte Citrix Scout.

O que é coletado

O 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 problemas 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 Rastreamento de Eventos para 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.
- Despejos de memória 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 na memória para evitar IOPs em máquinas provisionadas.

- O buffer de rastreamento usa um mecanismo circular para reter rastreamentos na memória.

O Call Home coleta os principais pontos de dados listados em Pontos de dados chave do Call Home.

Resumo de configuração e gerenciamento

Você pode se inscrever no Call Home ao usar o assistente de instalação do produto completo ou posteriormente, usando cmdlets do PowerShell. Ao se inscrever, por padrão, os diagnósticos são coletados e carregados para a Citrix todo domingo, aproximadamente às 3:00 AM, horário local. O upload é randomizado com um intervalo de duas horas a partir do horário especificado. Isso significa que um upload usando o agendamento padrão ocorre entre 3:00 AM e 5:00 AM.

Se você não quiser carregar informações de diagnóstico de forma agendada (ou se quiser alterar um agendamento), você pode usar cmdlets do PowerShell para coletar e carregar diagnósticos manualmente ou armazená-los localmente.

Ao se inscrever em uploads agendados do Call Home e ao carregar manualmente informações de diagnóstico para a Citrix, você fornece credenciais de conta Citrix ou Citrix Cloud™. A Citrix troca as credenciais por um token de upload que é usado para identificar o cliente e carregar os dados. As credenciais não são salvas.

Quando um upload ocorre, uma notificação é enviada por e-mail para o endereço associado à conta Citrix.

Se você habilitar o Call Home ao instalar um componente, poderá desativá-lo mais tarde.

Pré-requisitos

- A máquina deve estar executando o PowerShell 3.0 ou posterior.
- O Serviço de Telemetria Citrix deve estar em execução na máquina.
- A variável de sistema `PSModulePath` deve ser definida para o caminho de instalação da Telemetria, por exemplo, `C:\Program Files\Citrix\Telemetry Service\`.

Habilitar o Call Home durante a instalação do componente

Durante a instalação ou atualização do VDA: Ao instalar ou atualizar um Virtual Delivery Agent usando a interface gráfica no instalador do produto completo, 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 todas as quartas-feiras 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 de telemetria do PowerShell.)

```
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 **Off** 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.

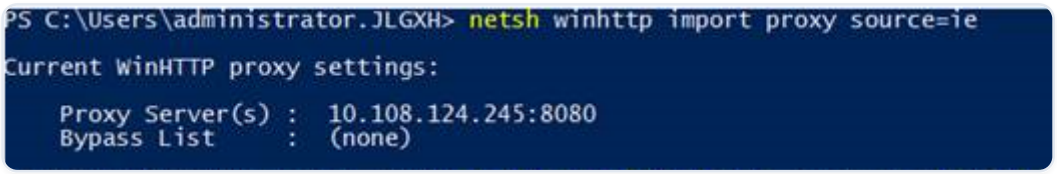
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:
\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

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 habilitado. Os diagramas de exemplo no procedimento a seguir contêm o endereço do servidor e a porta 10.158.139.37:3128. Suas informações serão diferentes.

1. Adicione informações do servidor proxy no 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 e o número da porta do servidor proxy.
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 então navegar até o local dos seus dados.

O CIS oferece suporte a vários cmdlets do PowerShell que gerenciam uploads de dados. Esta documentação aborda os cmdlets para dois casos comuns:

- Use o cmdlet `Start-CitrixCallHomeUpload` para coletar e carregar manualmente um pacote de informações de diagnóstico para o CIS. (O pacote não é salvo localmente.)
- Use o cmdlet `Start-CitrixCallHomeUpload` para coletar dados manualmente e armazenar um pacote de informações de diagnóstico localmente. Isso permite que você visualize os dados. Mais tarde, use o cmdlet `Send-CitrixCallHomeBundle` para carregar manualmente

uma cópia desse pacote para o CIS. (Os dados que você salvou originalmente permanecem localmente.)

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Ao inserir um cmdlet para carregar dados para o CIS, você será solicitado a confirmar o upload. Se o cmdlet expirar antes que o upload seja concluído, verifique o status do upload no log de eventos do sistema. A solicitação de upload pode ser rejeitada se o serviço já estiver realizando um upload.

Coletar dados e carregar pacote para o CIS:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

Coletar dados e salvá-los localmente:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

Os seguintes parâmetros são válidos:

- **Credencial:** 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 necessário ao salvar dados do Call Home localmente.
- **Descrição e Hora do Incidente:** Informações de formato livre sobre o upload.
- **SRNumber:** Número do incidente do Suporte Técnico Citrix.
- **Nome:** Nome que identifica o pacote.
- **UploadHeader:** String formatada em JSON especificando os cabeçalhos de upload carregados para o CIS.

- **AppendHeaders:** String formatada em JSON especificando os cabeçalhos anexados carregados para o CIS.
- **Coletar:** String formatada em JSON especificando quais dados coletar ou omitir, no formato {'collector':{'enabled':Boolean}}, onde Boolean é true ou false. Os valores de coletor válidos são:
  - 'WMI'
  - 'processo'
  - 'registro
  - 'relatório de falha'
  - 'rastreamento'
  - 'arquivo'
  - 'MSI'
  - 'dados locais'
  - 'dados do site'
  - 'SFB'

  Por padrão, todos os coletores, exceto 'sfb', estão habilitados.

  O coletor 'sfb' foi projetado para ser usado sob demanda para diagnosticar problemas do Skype for Business. Além do parâmetro 'enabled', o coletor 'sfb' suporta os parâmetros 'account' e 'accounts' para especificar usuários de destino. Use uma das formas:

  - "-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 seguinte cmdlet 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 seguinte cmdlet 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 seguinte cmdlet carrega o pacote de dados que você salvou anteriormente.

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

Citrix Scout

Introdução

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manter sua implantação do Citrix Virtual Apps and Desktops™. A Citrix oferece análise abrangente e automatizada de coletas de diagnóstico por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

Você pode carregar arquivos de coleta para a Citrix para análise e orientação do Suporte Citrix. Ou, você pode salvar uma coleta localmente para sua própria revisão e, posteriormente, 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 selecionar 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 selecionar. Em seguida, você recria os 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 selecionar. 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 forem encontrados problemas durante as verificações, o Scout fornece um relatório detalhado. Cada vez que o Scout é iniciado, 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 o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), execute o Scout a partir de um VDA para coletar diagnósticos locais.

O log para o aplicativo Scout é armazenado em `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Este arquivo pode ser usado para solução de problemas.

Assista a uma demonstração do Citrix Scout.

<iframe src="https://www.youtube.com/embed/2y9k07r8i0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

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 ao solucionar problemas comuns, como registros de VDA e inicializações de aplicativos/desktops. Nenhuma outra informação de Event Tracing for Windows (ETW) é coletada.

A coleta inclui:

- Entradas de registro criadas pelo Citrix Virtual Apps and Desktops em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informações do Windows Management Instrumentation (WMI) no **namespace Citrix**.
- Processos em execução.
- Dumps de falha de processos Citrix que são armazenados em `%PROGRAMDATA%\Citrix\CDF`.
- Informações de política Citrix, no formato CSV.
- Informações de instalação e atualização. A coleta pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront, logs de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

Sobre as informações de rastreamento:

- As informações de rastreamento são compactadas à medida que são coletadas, mantendo uma pequena pegada na máquina.

- Em cada máquina, o Serviço de Telemetria Citrix mantém informações de rastreamento recentes compactadas por um máximo de oito dias.
- A partir do Citrix Virtual Apps and Desktops 7 1808, os rastreamentos AOT são salvos no disco local por padrão. (Em versões anteriores, os rastreamentos eram mantidos na memória.) Caminho padrão = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partir do Citrix Virtual Apps and Desktops 7 1811, os rastreamentos AOT salvos em compartilhamentos de rede são coletados com outros diagnósticos.
- Você pode modificar o tamanho máximo (padrão = 10 MB) e a duração da fatia, usando o cmdlet `Enable-CitrixTrace` ou a string de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Os rastreamentos são anexados ao arquivo até que ele 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 até C:\Program Files\Citrix\Telemetry Service
2. Abra o arquivo ScoutUI.exe.config.
3. Altere o valor de LinuxVDATelemetryServicePort ou LinuxVDATelemetryWakeupPort para o que foi configurado no VDA Linux:

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. Salve as alterações e feche o arquivo.
2. Abra o Scout novamente para garantir que ele carregue a configuração mais recente.

Sobre 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.
- Existe apenas um Delivery Controller no site.
- Os Delivery Controllers são de versões diferentes.

Além de atender às permissões e requisitos para verificações de integridade, as verificações de configuração do Delivery Controller exigem:

- Pelo menos um Controller ligado.
- O Broker Service em execução em um Controller.
- Uma conexão de trabalho 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 de inicialização da sessão
- Status dos serviços de inicialização da sessão
- Configuração do firewall do Windows para inicialização da sessão
- Licenças de Acesso para Cliente dos Serviços de Área de Trabalho Remota do VDA
- Caminho de inicialização do aplicativo VDA
- Configurações de registro de inicialização da sessão

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 serviço Citrix Default Domain está em execução
- O serviço Citrix Credential Wallet está em execução

- Conexão do servidor StoreFront com a porta 88 do Active Directory
- Conexão do servidor StoreFront com a porta 389 do Active Directory
- A URL base tem um FQDN válido
- O endereço IP correto da URL base pode ser recuperado
- O pool de aplicativos do IIS está usando .NET 4.0
- Se o certificado está vinculado à porta SSL para a URL do host
- Se a cadeia de certificados está completa
- Se os certificados expiraram
- Se um certificado está expirando em breve (dentro de 30 dias)

Verificações do Servidor de Licenças

As verificações do Servidor de Licenças verificam:

- Conexão do Servidor de Licenças a partir do Delivery Controller
- Status de acesso remoto do firewall do Servidor de Licenças
- Status do serviço de Licenciamento Citrix
- Estado do 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 inicial, clique em **Verificação de Integridade**.
2. Selecione as máquinas. Clique em **Localizar máquina** para descobrir máquinas. A página **Selecionar máquinas** lista todos os VDAs, Delivery Controllers e Servidores de Licenças descobertos no site. Você pode filtrar a exibição por nome da máquina. 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 é exibida na coluna **Status** e a caixa de seleção dessa máquina é desmarcada. Você pode:

   - Resolver o problema e, em seguida, marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (deixe a caixa de seleção desmarcada). 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 foram 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 o fizer, os resultados da verificação serão perdidos.)

4. Quando as verificações forem concluídas, clique em **Concluído** para retornar à página inicial do Scout.

Resultados da verificação de integridade

Para verificações Citrix que geram relatórios, os relatórios contêm:

- Hora e data em que o relatório de resultados foi gerado
- Máquinas que foram verificadas
- Condições que a verificação procurou nas máquinas de destino

Permissões e requisitos

Permissões:

- Para coletar diagnósticos:
  - Você deve ser um administrador local e usuário de domínio para cada máquina da qual você está coletando diagnósticos.
  - Você deve ter permissão para gravar no diretório LocalAppData em cada máquina.
- Para executar verificações de integridade:
  - Você deve ser um membro do grupo de usuários do domínio.
  - Você deve ser um administrador completo ou ter uma função personalizada com permissões somente leitura e de **Executar Testes de Ambiente** para o site.
  - Defina a política de execução de script para pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** outros privilégios de execução de script também podem funcionar.
- Use **Executar como administrador** ao iniciar o Scout.

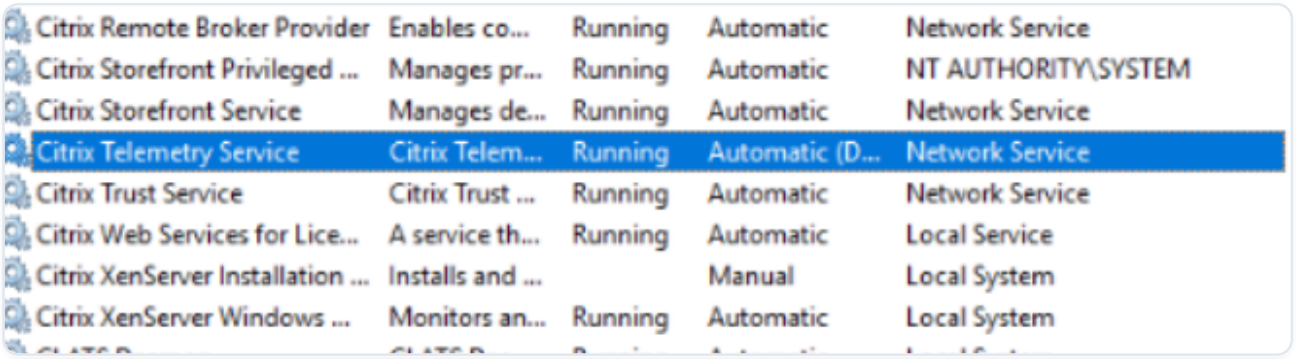
Para cada máquina da qual você coleta diagnósticos ou executa verificações de integridade:

- O Scout deve ser capaz de se comunicar com a máquina.
- O compartilhamento de arquivos e impressoras deve estar ativado.
- PSRemoting e WinRM devem estar habilitados. A máquina também deve estar executando o PowerShell 3.0 ou posterior.
- O Citrix Telemetry Service 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.

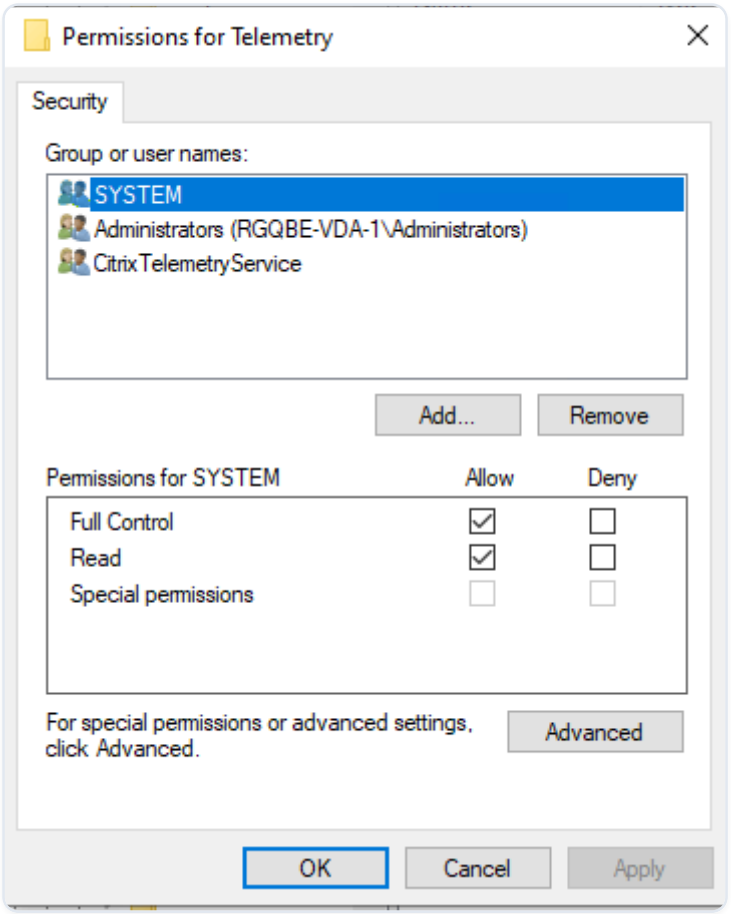
O Scout executa testes de verificação nas máquinas que você seleciona, para garantir que esses requisitos sejam atendidos.

O Telemetry Service para Windows é executado no Network Service.

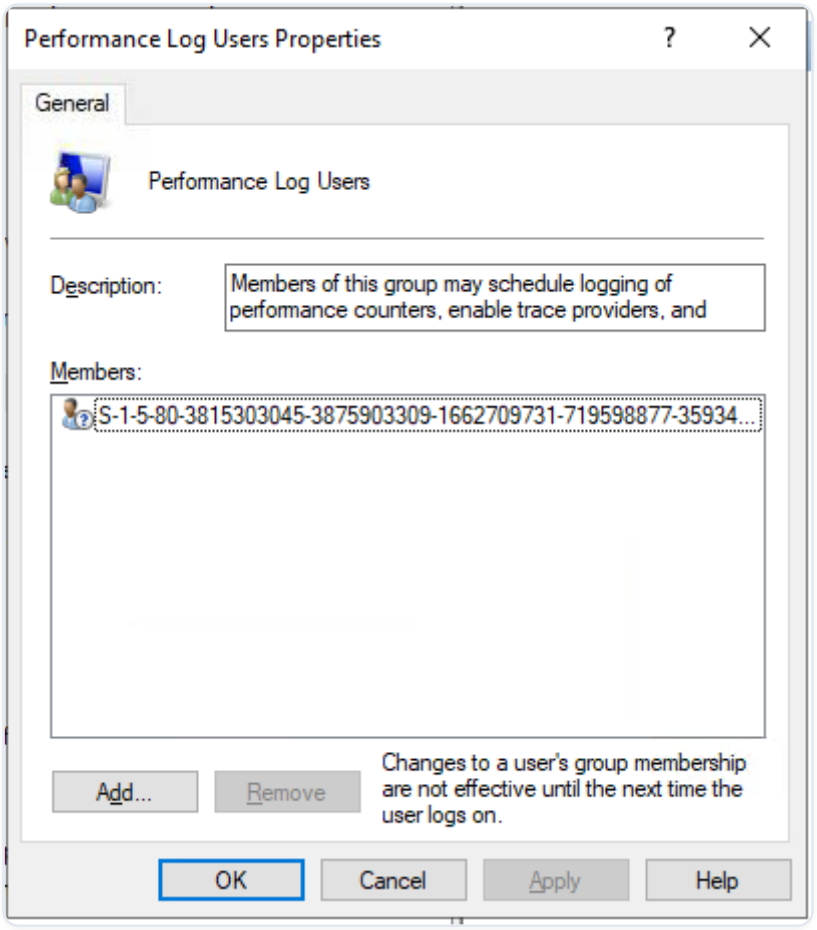


A pasta de rastreamento AOT é salva em `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Somente usuários no grupo Administrador, Sistema e SID do Telemetry Service têm permissão para acessar o registro `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.



O SID do Telemetry Service permanece no grupo Performance Log Users após a desinstalação do Telemetry Service, mas você pode removê-lo manualmente.



Testes de verificação

Antes do início de uma coleta de diagnóstico ou verificação de integridade, os 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.

- **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 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 do VDA Linux não está iniciado nesta máquina** - Certifique-se de que:
  - A porta 7502 está aberta. Verifique se o Serviço de Telemetria do VDA Linux está instalado e iniciado na máquina. A porta pode ser diferente se a porta do serviço de telemetria tiver sido alterada. Consulte Configuração do Scout para ajustar as portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)

Compatibilidade de versão

Esta versão do Scout (3.x) destina-se a ser executada em Controladores e VDAs do Citrix Virtual Apps and Desktops (ou mínimo XenApp e XenDesktop 7.14).

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 Sempre Ativos (AOT)	Não	Sim
Permitir a coleta de dados de diagnóstico	Até 10 máquinas de uma vez (por padrão)	Ilimitado (sujeito à disponibilidade de recursos)
Permitir que os dados de diagnóstico sejam enviados para a Citrix	Sim	Sim
Permitir que os 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

RECURSO	SCOUT 2.23	SCOUT 3.0
Suporte a script	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 de 3.17

Instalar e atualizar

Por padrão, o Scout é instalado ou atualizado automaticamente como parte do Serviço de Telemetria Citrix quando você instala ou atualiza um VDA ou um Controller.

Se você omitir o Serviço de Telemetria Citrix ao instalar um VDA, ou remover o serviço posteriormente, execute `TelemetryServiceInstaller_xx.msi` da pasta `x64\Virtual Desktop Components` ou `x86\Virtual Desktop Components` na mídia de instalação do Citrix Virtual Apps and Desktops.

Ao selecionar a ação **Coletar** ou **Rastrear e Reproduzir**, você será notificado se uma máquina estiver executando uma versão mais antiga do Serviço de Telemetria Citrix. A Citrix recomenda usar a versão mais recente suportada. Se você não atualizar o Serviço de Telemetria nessa máquina, ele não será incluído nas ações **Coletar** ou **Rastrear e Reproduzir**. Para atualizar o Serviço de Telemetria, use o mesmo procedimento de instalação.

Autorização de upload

Se você planeja fazer upload de coleções de diagnóstico para a Citrix, você deve ter uma conta Citrix ou Citrix Cloud. (Estas são as credenciais que você usa para acessar downloads da Citrix ou acessar o Citrix Cloud Control Center.) Após a validação das suas credenciais de conta, um token é emitido.

- Se você autenticar com uma conta Citrix, o processo de emissão de token não é visível. Você simplesmente insere suas credenciais de conta. Depois que a Citrix valida as credenciais, você pode continuar no assistente do Scout.
- Se você autenticar com uma conta Citrix Cloud, você clica 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, você pode instruir o Scout a usar as configurações de proxy configuradas nas Propriedades da Internet do seu navegador. Alternativamente, você pode especificar o endereço IP e o número da porta do servidor proxy.

Localizar máquina

Para os procedimentos **Coletar**, **Rastrear e Reproduzir** e **Agendar**, o Scout lista os Controllers e VDAs que ele descobre automaticamente.

Quando você executa Scout Health Check a partir do Delivery Controller, clique em **Localizar máquina** para descobrir máquinas, incluindo controladores de entrega, VDAs, servidores de licença e servidores StoreFront.

Quando você executa o Scout Health Check a partir de uma máquina ingressada no domínio que não é um Delivery Controller, o Scout não consegue descobrir máquinas automaticamente. Você precisa adicionar máquinas manualmente ou importar máquinas VDA.

Adicionar máquinas manualmente

Depois que o Scout lista os Controladores e VDAs que ele descobre, você pode adicionar manualmente outras máquinas na implantação, como servidores StoreFront, Servidores de Licença e servidores Citrix Provisioning.

Ao executar verificações de integridade:

- Os Servidores de Licença Citrix no domínio são descobertos automaticamente. Você não pode adicionar Servidores de Licença manualmente.
- As verificações de integridade não suportam atualmente servidores Citrix Provisioning.

Em qualquer página do Scout que liste as máquinas descobertas, clique em **+ Adicionar máquina**. Digite o FQDN da máquina que você deseja adicionar e, em seguida, clique em

Continuar. Repita para adicionar outras máquinas, conforme necessário. (Embora inserir um alias DNS em vez de um FQDN possa parecer válido, as verificações de integridade podem falhar.)

As máquinas adicionadas manualmente sempre aparecem no topo da lista de máquinas, acima das máquinas descobertas.

Uma maneira fácil de identificar uma máquina adicionada manualmente é o botão vermelho de exclusão no lado direito da linha. Somente as máquinas adicionadas manualmente têm esse botão. As máquinas descobertas não têm.

Para remover uma máquina adicionada manualmente, clique no botão vermelho no lado direito da linha. Confirme a exclusão. Repita para excluir outras máquinas adicionadas manualmente.

O Scout lembra as máquinas adicionadas manualmente até que você as remova. Quando você fecha e reabre o Scout, as máquinas adicionadas manualmente ainda são listadas no topo da lista.

Os rastreamentos CDF não são coletados ao usar **Rastrear e Reproduzir** em servidores StoreFront. No entanto, todas as outras informações de rastreamento são coletadas.

Importar máquinas VDA

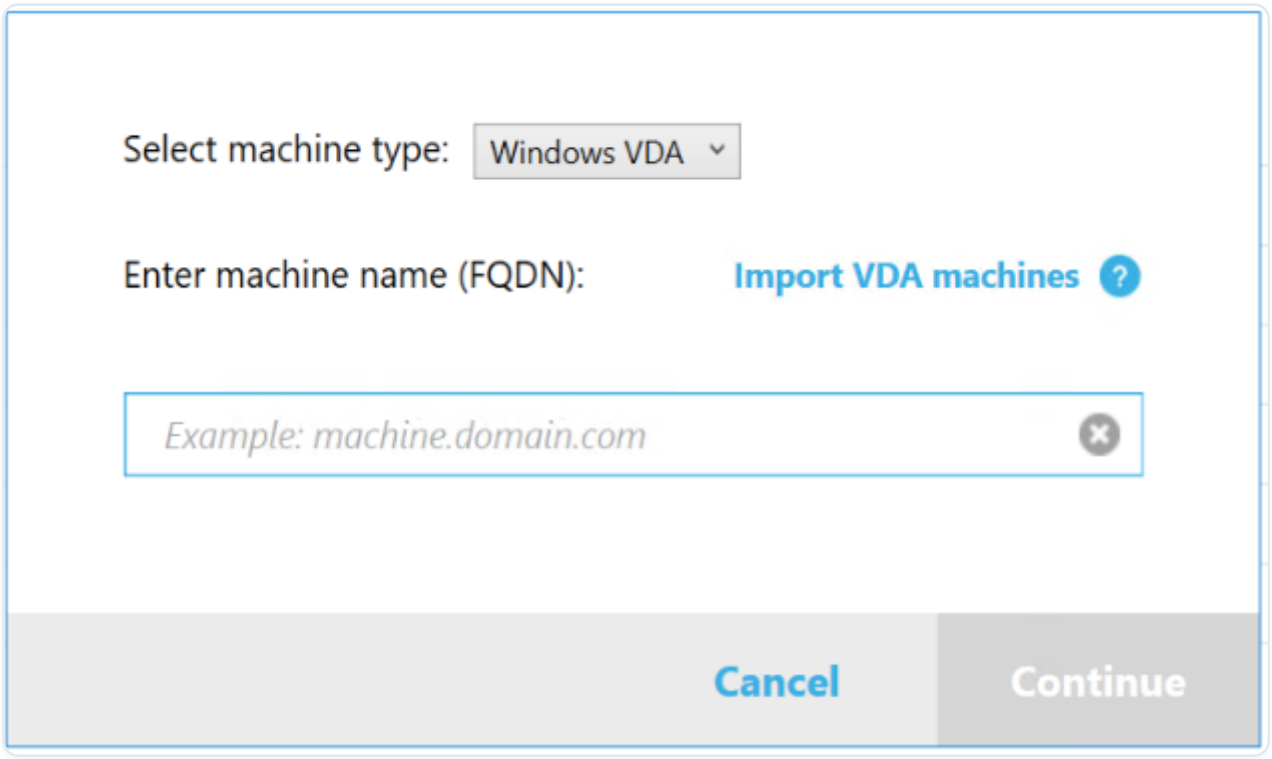
Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

1. No Delivery Controller ou Connector, gere o arquivo de lista de máquinas com o comando PowerShell. No Connector, você deve inserir as credenciais da 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 onde você deseja iniciar o Scout Health Check.
3. Na página Scout Health Check, clique em **Adicionar Máquina**.
4. Selecione o tipo de máquina **Windows VDA**.
5. Clique em **Importar máquinas VDA**.
6. Selecione o arquivo machineList.txt.
7. Clique em **Abrir**.

As máquinas VDA importadas são listadas na página Scout Health Check.



Coletar diagnósticos

O procedimento de **Coleta** compreende a seleção de máquinas, o início da coleta de diagnósticos e, em seguida, o upload do arquivo contendo a coleta para a Citrix ou o salvamento local.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, 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.

   Selecione a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar, uma mensagem será exibida na coluna **Status** e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolver o problema e, em seguida, selecionar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignorar essa máquina (deixe 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 **Repetir** na coluna **Ação** para cada máquina.
   - Quando a coleta for concluída para todas as máquinas selecionadas, o botão **Parar Coleta** no canto inferior direito mudará para **Continuar**.
   - Para coletar diagnósticos novamente, clique em **Coletar Novamente** na coluna **Ação** dessa máquina. A coleta mais recente sobrescreve a anterior.
   - Se uma coleta falhar, você pode clicar em **Repetir** na coluna **Ação**. Somente 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 clicar, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

4. Salvar ou carregar a coleção. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo na máquina local.

   Se você optar por carregar o arquivo agora, continue com a Etapa 5.

   Se você optar por salvar o arquivo localmente:

   - Uma caixa de diálogo **Salvar** do Windows é exibida. navegar até o local desejado.

- Quando o salvamento local for concluído, o caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Você pode carregar o arquivo mais tarde para a Citrix. Consulte CTX136396.

Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir mais nenhuma etapa neste procedimento.

5. autenticar para uploads e, opcionalmente, especifique um proxy. Para obter detalhes, consulte Autorização de upload.

   - Se você não se autenticou pelo Scout, continue com esta etapa.
   - Se você se autenticou pelo Scout, o token de autorização armazenado é usado por padrão. Se for isso que você deseja fazer, selecione esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleção. Continue com a Etapa 6.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você 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 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 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.

Rastrear e reproduzir

O procedimento **Rastrear e Reproduzir** compreende a seleção de máquinas, o início de um rastreamento, a reprodução de problemas, a conclusão da coleta de diagnósticos e, em seguida, o upload do arquivo para a Citrix ou o salvamento localmente.

Este procedimento é semelhante ao procedimento padrão de **Coleta**. No entanto, ele permite que você inicie um rastreamento em máquinas e, em seguida, recrie problemas nessas máquinas. Todas as coletas de diagnóstico incluem informações de rastreamento AOT. Este procedimento adiciona rastreamentos CDF para 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. Marque a caixa de seleção ao lado de cada máquina da qual você 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 é exibida na coluna **Status**, e a caixa de seleção dessa máquina é desmarcada. Você pode:

   - Resolva o problema e, em seguida, selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.

- Ignore essa máquina (deixe sua caixa de seleção desmarcada). Diagnósticos e rastreamentos não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

3. Inicie o rastreamento. O resumo lista todas as máquinas das quais os rastreamentos são coletados. Clique em **Iniciar Rastreamento**.

   Em uma ou mais das máquinas selecionadas, reproduza os problemas que você encontrou. A coleta de rastreamento continua enquanto você faz isso. Quando terminar de reproduzir o problema, clique em **Continuar** no Scout. Isso interrompe o rastreamento.

   Depois de interromper o rastreamento, indique se você reproduziu o problema durante o rastreamento.

4. Colete diagnósticos das máquinas. Clique em **Iniciar Coleta**. Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta para uma máquina.
   - Para interromper uma coleta em andamento em uma única máquina, clique em **Cancelar** na coluna **Ação** para essa máquina.
   - Para interromper todas as coletas em andamento, clique em **Parar Coleta** no canto inferior direito da página. Os diagnósticos das máquinas que concluíram a coleta são mantidos. Para retomar a coleta, clique em **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 coletas bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Voltar**. (Se você fizer isso, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

5. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo localmente.

   Se você optar por carregar o arquivo agora, continue com a Etapa 6.

   Se você optar por salvar o arquivo localmente:

   - Uma caixa de diálogo Salvar do Windows é exibida. Selecione o local desejado.

- Quando o salvamento local for concluído, o caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Lembre-se: você pode carregar o arquivo mais tarde da Citrix; consulte CTX136396 para Citrix Insight Services.

Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir mais nenhuma etapa neste procedimento.

6. autenticar para uploads e, opcionalmente, especifique o proxy. Revise Autorização de upload para obter detalhes deste processo.

   - Se você não se autenticou pelo Scout, continue com esta etapa.
   - Se você se autenticou pelo Scout, o token de autorização armazenado é usado por padrão. Se é isso que você deseja fazer, escolha esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleta. Continue com a Etapa 7.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você deseja usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será iniciado em uma página do Citrix Cloud onde um token é exibido. Copie o token e, em seguida, cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

7. Forneça informações sobre o upload.

   Insira os detalhes do upload:

   - O campo de nome contém o nome padrão para o arquivo dos diagnósticos coletados. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo de nome vazio, o nome padrão será usado.)

- Opcionalmente, especifique um número de caso de suporte Citrix de 8 dígitos.
- No campo opcional Descrição, descreva o problema e indique quando o problema ocorreu, se aplicável.

Quando terminar, clique em **Iniciar Upload**.

Durante o upload, a parte inferior esquerda da página mostra aproximadamente qual porcentagem do upload 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. Iniciar 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 no ícone de 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 consiste em selecionar máquinas e, em seguida, definir ou cancelar o agendamento. As coletas agendadas são automaticamente carregadas para a Citrix. (Você pode salvar as 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.

   Quando você instalou VDAs e Controladores usando a interface gráfica, se você definiu um agendamento de Call Home (consulte Citrix Call Home), o Scout exibe essas configurações por padrão. Você pode usar esta versão do Scout para iniciar coletas agendadas pela primeira vez ou alterar um agendamento configurado anteriormente.

   Embora você tenha ativado/desativado o Call Home por máquina durante a instalação do componente, um agendamento configurado no Scout afeta todas as máquinas que você selecionar.

   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 ela atenda aos critérios em Testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será postada na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

   - Resolver o problema e, em seguida, marcar 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 serão 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 (relógio de 24 horas) para o início da coleta.
   - Para configurar um agendamento diário para as máquinas selecionadas, clique em **Diário**. Insira a hora do dia (relógio de 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. Consulte Autorização de upload para obter detalhes sobre esse 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 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 aberto em uma página do Citrix Cloud onde um token é exibido. Copie o token e cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

   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 hipervisores, 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 coleção de diagnósticos.
    - Se você selecionar **Carregar a coleção de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleção de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

Executar mascaramento de dados em diagnósticos existentes

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório onde o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie o Scout diretamente no modo de mascaramento de dados: `ScoutUI.exe datamasking filePath`.
4. Selecione “Habilitar mascaramento de dados” para continuar. Esta opção está habilitada por padrão.

5. Configure a máscara de dados. Você pode executar o mascaramento de dados com as regras padrão ou personalizar as regras.
6. Selecione se deseja carregar ou salvar a coleção de diagnósticos.
    - Se você selecionar **Carregar a coleção de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleção de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

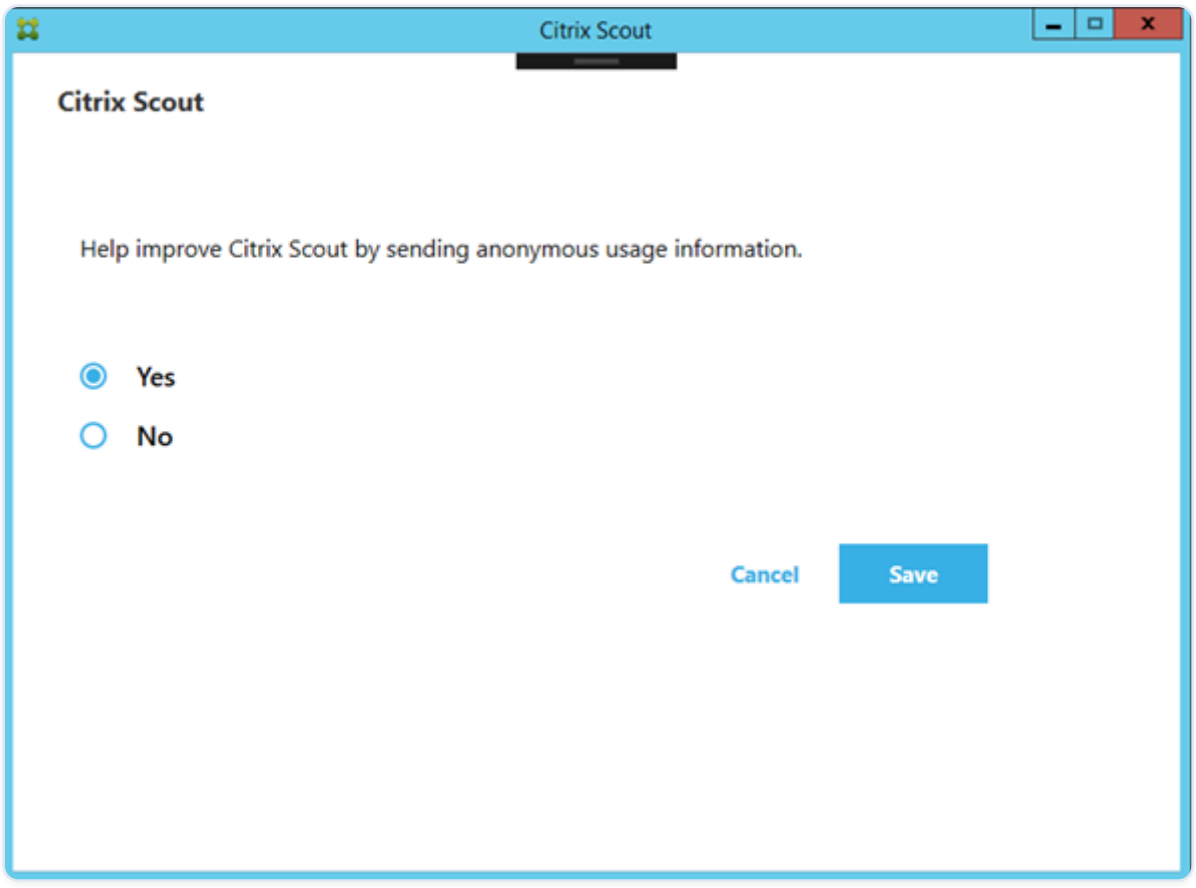
Locais do arquivo de dados mascarados e do arquivo de mapeamento

Depois de carregar ou salvar a coleção de diagnósticos, clique no link para abrir os diagnósticos originais e mascarados, e abra o arquivo de informações de mapeamento.

Coleta de dados de uso

Ao usar o Scout, a Citrix usa o Google Analytics para coletar dados de uso anônimos que serão utilizados para futuros recursos e melhorias do produto. A coleta de dados é habilitada por padrão.

Para alterar a coleta e o upload de dados de uso, clique no ícone de engrenagem **Configurações** na interface do usuário do Scout. Você pode então escolher se deseja enviar as informações selecionando **Sim** ou **Não** e, em seguida, clicando em **Salvar**.



Principais pontos de dados do Call Home

O Call Home coleta os seguintes principais pontos de dados.

(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 do Broker (M)
		Instâncias de Serviço Registradas (M)
		Teste de Licença do Broker (M)
		Sessão HDX™ Ativa (M)
		Administrador do Broker
		Permissão de Administrador do Broker
		Configuração RDS (inclui LicensingSettings, SessionSettings, SpecifiedLicenseServers e RegisteredLicenseServers)

		Serviço de Monitoramento (M) (inclui MonitorConfiguration, MonitorDataStore, MonitorDBConnection, MonitorDBSchemaVersion, MonitorService, MonitorServiceAddedCapability, MonitorServiceInstance, MonitorServiceStatus e MonitorInstalledDBVersion)
		Registro de Configuração
		Log de Conexão
		Conexões de Hypervisor (M)
		Conexão de Hypervisor do Broker
		Alertas de Hypervisor
		Catálogos
		Agentes de SO multi-sessão (M)
		Agentes de SO de sessão única (M)
		Aplicativos Publicados
		Grupos de Entrega
		Agentes de Entrega Configurados

		Componentes Instalados Citrix

		Informações do Serviço de Broker Citrix
		Arquivo de configuração do Serviço de Broker
		Arquivo de configuração do Machine Creation Services™
		Arquivo de configuração do Serviço de Host
		Arquivo de configuração do Serviço de Identidade AD
		Arquivo de configuração do Serviço de Configuração
		Arquivo de configuração do Serviço de Log de Configuração
		Arquivo de configuração do Serviço de Administração Delegada
		Arquivo de configuração do Serviço de Teste de Ambiente
		Arquivo de configuração do Serviço de Monitoramento
		Arquivo de configuração do Serviço Storefront™
		Arquivo de configuração do Agente da Estação de Trabalho
		Informações do VDA Citrix
		Hotfix Citrix XD

		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		Computador
		BIOS
		Informações 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)
		Dumps de Falha

		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 Ativado
		Experiência Clássica Ativada para Citrix Receiver™
		Configuração do Receiver HTML5 para Citrix Receiver
		Controle de Workspace Ativado para Citrix Receiver
		Acesso Remoto Ativado para Loja
		Contagem de Gateways
		Serviço JSON explícito para autenticação NetScaler® integrada

Monitor

Administradores e pessoal de suporte técnico 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 Director.

Registro de Configuração

O Registro de Configuração permite que os administradores acompanhem as alterações administrativas em um Site. O Registro de Configuração pode ajudar os administradores a diagnosticar e solucionar problemas após a realização de alterações de configuração, auxiliar no gerenciamento de mudanças e rastrear configurações, e relatar a atividade de administração.

Você pode visualizar e gerar relatórios sobre informações registradas no Studio. Você também pode visualizar itens registrados no Director com a Visualização de Tendências para fornecer notificações de alterações de configuração. Este recurso é útil para administradores que não têm acesso ao Studio.

A Visualização de Tendências fornece dados históricos de alterações de configuração ao longo de um período de tempo para que os administradores possam avaliar quais alterações foram feitas

no Site, quando foram feitas e quem as fez para encontrar a causa de um problema. Esta visualização classifica as informações de configuração em três categorias:

- Falhas de Conexão
- Máquinas de sessão única com falha
- Máquinas multissessão com falha

Para obter detalhes sobre como habilitar e configurar o Log de Configuração, consulte Log de Configuração. Os artigos do Director descrevem como visualizar as informações registradas a partir dessa ferramenta.

Logs de eventos

Os serviços 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 alterações de configuração do site e atividades administrativas para o banco de dados. O recurso é habilitado por padrão. Você pode usar o conteúdo registrado para:

- Diagnosticar e solucionar problemas após a realização de alterações de configuração. O log fornece um rastro de auditoria.
- Auxiliar no gerenciamento de mudanças e rastrear configurações.
- Relatar a atividade de administração.

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 de 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 gerenciamento de pool de inicialização de máquinas virtuais.
- Ações de política implementadas por meio do Console de Gerenciamento de Política de Grupo (GPMC); use ferramentas da Microsoft para visualizar 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 que é criado quando você cria 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 adversamente o espaço disponível para o banco de dados de configuração do site.
- Ele 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 habilitado e o registro obrigatório está desabilitado.

1. Selecione **Registro** no painel de navegação do Studio.
2. Selecione **Preferências** no painel 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 habilitados ou desabilitados.
3. Selecione a ação desejada:

   Para habilitar o registro de configuração, selecione **Habilitar**. Esta é a configuração padrão. Se não for possível gravar no banco de dados, as informações de registro serão descartadas, mas a operação continuará.

   Para desabilitar o registro de configuração, selecione **Desabilitar**. Se o registro estava habilitado anteriormente, os logs existentes permanecem legíveis com o SDK do PowerShell.

Para habilitar o registro obrigatório, selecione **Impedir alterações na configuração do site quando o banco de dados não estiver disponível**. Nenhuma alteração de configuração ou atividade administrativa que normalmente é registrada é permitida, a menos que possa ser gravada no banco de dados de registro de configuração. Você pode habilitar o registro obrigatório somente quando o registro de configuração estiver habilitado (quando **Habilitar** estiver selecionado). Se o Serviço de Registro de Configuração falhar e a alta disponibilidade não estiver em uso, o registro obrigatório será assumido. Nesses casos, as operações que normalmente seriam registradas não são executadas.

Para desabilitar o registro obrigatório, selecione **Permitir alterações na configuração do site quando o banco de dados não estiver disponível**. As alterações de configuração e as atividades administrativas são permitidas, mesmo que o banco de dados de registro de configuração não possa ser acessado. Esta é a configuração padrão.

Alterar o local do banco de dados de registro de configuração

Não é possível alterar o local do banco de dados quando o registro obrigatório está habilitado, porque a alteração de local inclui um breve intervalo de desconexão que não pode ser registrado.

1. Crie um servidor de banco de dados, usando uma versão compatível do SQL Server.
2. Selecione **Registro** no painel de navegação do Studio.
3. Selecione **Preferências** no painel 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 a base de dados, clique em **OK**. Quando solicitado, clique em **OK**, e o banco de dados será criado automaticamente. O Studio tenta acessar a base de dados usando as credenciais do usuário atual do Studio. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. O Studio então carrega o esquema da base de dados para ela. (As credenciais são retidas apenas durante a criação do banco de dados.)
7. Para criar o banco de dados manualmente, clique em **Gerar script de banco de dados**. O script gerado inclui instruções para criar o banco de dados manualmente. Certifique-se de que o banco de dados esteja vazio e que pelo menos um usuário tenha permissão para acessar e alterar o banco de dados antes de carregar o esquema.

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

Exibir conteúdo do log de configuração

Ao iniciar alterações de configuração e atividades administrativas, as operações de alto nível criadas pelo Studio e Director são listadas no painel superior central do Studio. Uma operação de alto nível resulta em uma ou mais chamadas de serviço e SDK, que são operações de baixo nível. Ao selecionar uma operação de alto nível no painel superior, o painel inferior exibe as operações de baixo nível.

Se uma operação falhar antes da conclusão, a operação de log pode não ser concluída no banco de dados. Por exemplo, um registro de início não terá um registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Ao exibir logs com base em intervalos de tempo, logs incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se todos os logs dos últimos cinco dias forem solicitados e um log existir com um horário de início nos últimos cinco dias, mas não tiver um horário de término, ele será incluído.

Ao usar um script que chama cmdlets do PowerShell, se você criar uma operação de baixo nível sem especificar uma operação de alto nível pai, o log de configuração criará uma operação de alto nível substituta.

Para exibir o conteúdo do log de configuração, selecione **Registro** no painel de navegação do Studio. Por padrão, o painel central lista o conteúdo do log cronologicamente (entradas mais recentes primeiro), separado por data. Você pode:

- Classificar a exibição pelo cabeçalho da coluna.
- Filtrar a exibição especificando um intervalo de dias ou inserindo texto na caixa **Pesquisar**. Para retornar à exibição padrão após usar a pesquisa, limpe o texto na caixa **Pesquisar**.

Gerar relatórios

Você pode gerar relatórios CSV e HTML contendo dados de log de configuração.

- O relatório CSV contém todos os dados de log de um intervalo de tempo especificado. Os dados hierárquicos no banco de dados são nivelados em uma única tabela CSV. Nenhum aspecto dos dados tem precedência no arquivo. Nenhuma formatação é usada e nenhuma legibilidade humana é assumida. O arquivo (nomeado MyReport) contém os dados em um formato universalmente consumível. Arquivos CSV são frequentemente usados para arquivar

dados ou como fonte de dados para uma ferramenta de relatório ou manipulação de dados, como o Microsoft Excel.

- O relatório HTML fornece uma forma legível por humanos dos dados de log para um intervalo de tempo especificado. Ele oferece uma visualização estruturada e navegável para revisar as alterações. Um relatório HTML é composto por dois arquivos, chamados Resumo e Detalhes. O Resumo lista as operações de alto nível: quando cada operação ocorreu, por quem e o resultado. Clicar em um link **Detalhes** ao lado de cada operação leva você às operações de baixo nível no arquivo Detalhes, que fornece informações adicionais.

Para gerar um relatório de log de configuração, selecione **Registro** no painel de navegação do Studio e, em seguida, selecione **Criar relatório personalizado** no painel Ações.

- Selecione o intervalo de datas para o relatório.
- Selecione o formato do relatório: CSV, HTML ou ambos.
- Navegue até o local onde deseja salvar o relatório.

Excluir conteúdo do log de configuração

Para excluir o log de configuração, você deve ter certas permissões de administração delegada e de banco de dados do SQL Server.

- **Administração delegada:** Você deve ter uma função de administração delegada que permita a leitura da configuração da implantação. A função de administrador completo tem essa permissão. Uma função personalizada deve ter Somente leitura ou Gerenciar selecionado na categoria Outras permissões.

  Para criar um backup dos dados de log de configuração antes de excluí-los, a função personalizada também deve ter Somente leitura ou Gerenciar selecionado na categoria Permissões de log.
- **Banco de dados SQL Server:** Você deve ter um login de servidor SQL com permissão para excluir registros do banco de dados. Existem duas maneiras de fazer isso:
  - Use um login de banco de dados do SQL Server com uma função de servidor sysadmin, que permite realizar qualquer atividade no servidor de banco de dados. Alternativamente, as funções de servidor `serveradmin` ou `setupadmin` permitem 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. Selecione **Registro** no painel de navegação do Studio.
2. Selecione **Excluir logs** no painel Ações.
3. Será perguntado se você deseja criar um backup dos logs antes que sejam excluídos. Se você optar por criar um backup, navegue até o local onde o arquivo de backup será salvo. O backup é criado como um arquivo CSV.

Depois que os logs de configuração são limpos, a exclusão do log é a primeira atividade registrada no log vazio. Essa entrada fornece detalhes sobre quem excluiu os logs e quando.

Logs de eventos

Os artigos a seguir listam e descrevem eventos que podem ser registrados por 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 Serviço de Broker do Citrix
- Eventos do SDK do Serviço FMA do Citrix
- Eventos do Serviço de Configuração do Citrix
- Eventos do Serviço de Administração Delegada do Citrix

Director

Director é um console de monitoramento e solução de problemas para Citrix Virtual Apps and Desktops.

Arquitetura do Director(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/director-architecture.png)

O Director pode acessar:

- Dados em tempo real do Broker Agent usando um console unificado integrado com Analytics, Performance Manager e Network Inspector. As seguintes análises são fornecidas pelo Citrix ADM para identificar gargalos devido à rede em seu ambiente Citrix Virtual Apps™ ou Desktops:
    - Gerenciamento de desempenho para garantia de integridade e capacidade
    - Análise de tendências históricas e de rede
- Dados históricos armazenados no banco de dados do Monitor para acessar o banco de dados de Log de Configuração.
- 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. Este 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 impactar o desempenho do SQL Server. Para obter mais informações, consulte o artigo de suporte da Microsoft, Proteja o SQL Server contra ataques de vulnerabilidades de canal lateral Meltdown e Spectre. 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

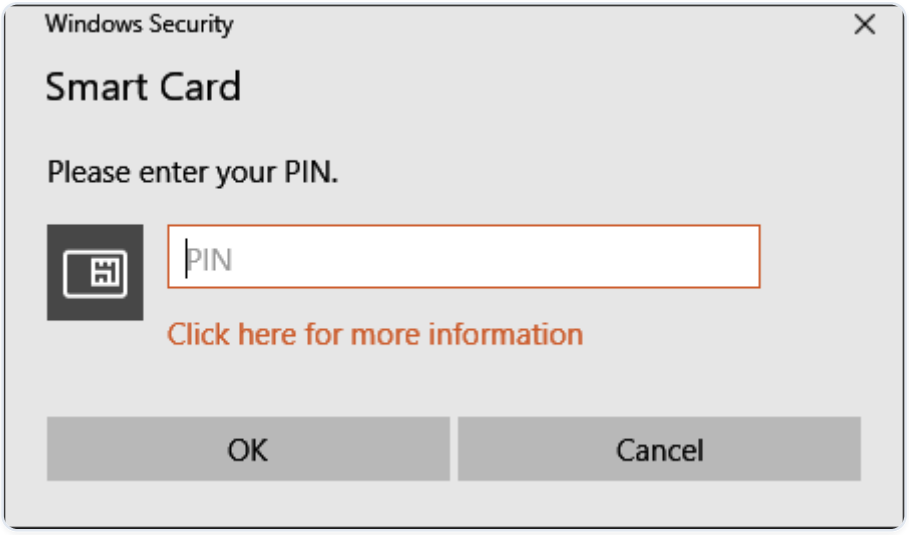
O Director agora oferece suporte à autenticação de cartão inteligente baseada em Verificação de Identidade Pessoal (PIV) para logon. Esse recurso é útil para organizações e agências governamentais que usam autenticação baseada em cartão inteligente para controle de acesso. A autenticação de cartão inteligente 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. Depois de autenticado, você pode acessar o Director sem precisar digitar credenciais adicionais na página de logon do Director.

Usar o Director com Autenticação Integrada do Windows

Com a Autenticação Integrada do Windows (IWA), os usuários ingressados no domínio obtêm acesso direto ao Director sem precisar 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 por 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 por Formulários deve permanecer definida como Habilitada para a autenticação de usuários não-domínio.

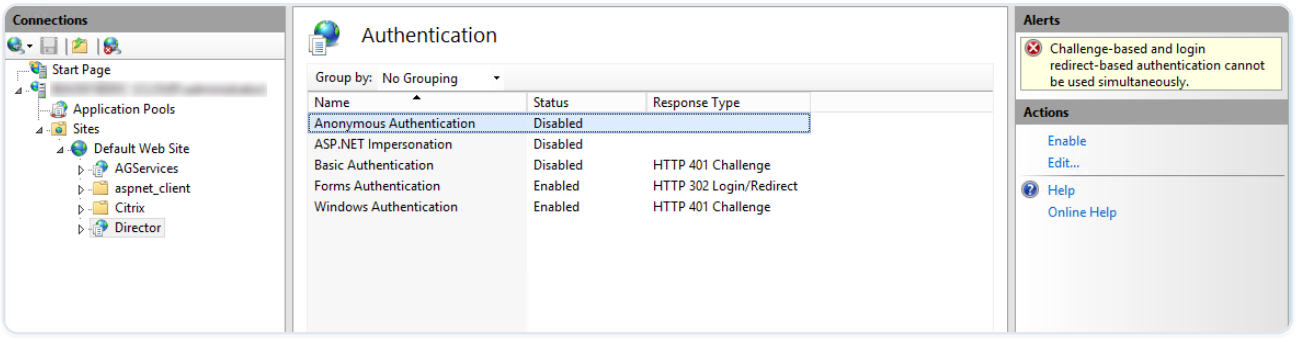
  a. Inicie o gerenciador do IIS.

  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 até **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 oferecer suporte à 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 como **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 realizando ações como encerrar um aplicativo ou processo que não responde, sombrear operações na máquina do usuário, reiniciar a máquina ou redefinir o perfil do usuário.

Em contraste, os administradores completos veem e gerenciam todo o Site e podem executar comandos para vários usuários e máquinas. O Painel fornece uma visão geral dos principais aspectos de uma implantação, como o status das sessões, logons de usuários e a infraestrutura do Site. As informações são atualizadas a cada minuto. Se ocorrerem problemas, os detalhes sobre o número e o tipo de falhas que ocorreram aparecerão automaticamente.

Para obter mais informações sobre as várias funções e suas permissões no Director, consulte Administração Delegada e Director

Coleta de dados de uso pelo Google Analytics

O Serviço Director começa a usar o Google Analytics para coletar dados de uso após a instalação do Director. Estatísticas sobre o uso das páginas de Tendências e análises de chamadas da API OData são coletadas. A coleta de análises está em conformidade com a Política de Privacidade da Citrix. A coleta de dados é habilitada por padrão quando você instala o Director.

Para desativar a coleta de dados do 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 com o valor desejado. Atualize a instância do Director após alterar o valor da chave do registro.

Cuidado: O uso incorreto do Editor do Registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

Local: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGoogleAnalytics

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 geral dos 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.

> Localização: 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



```

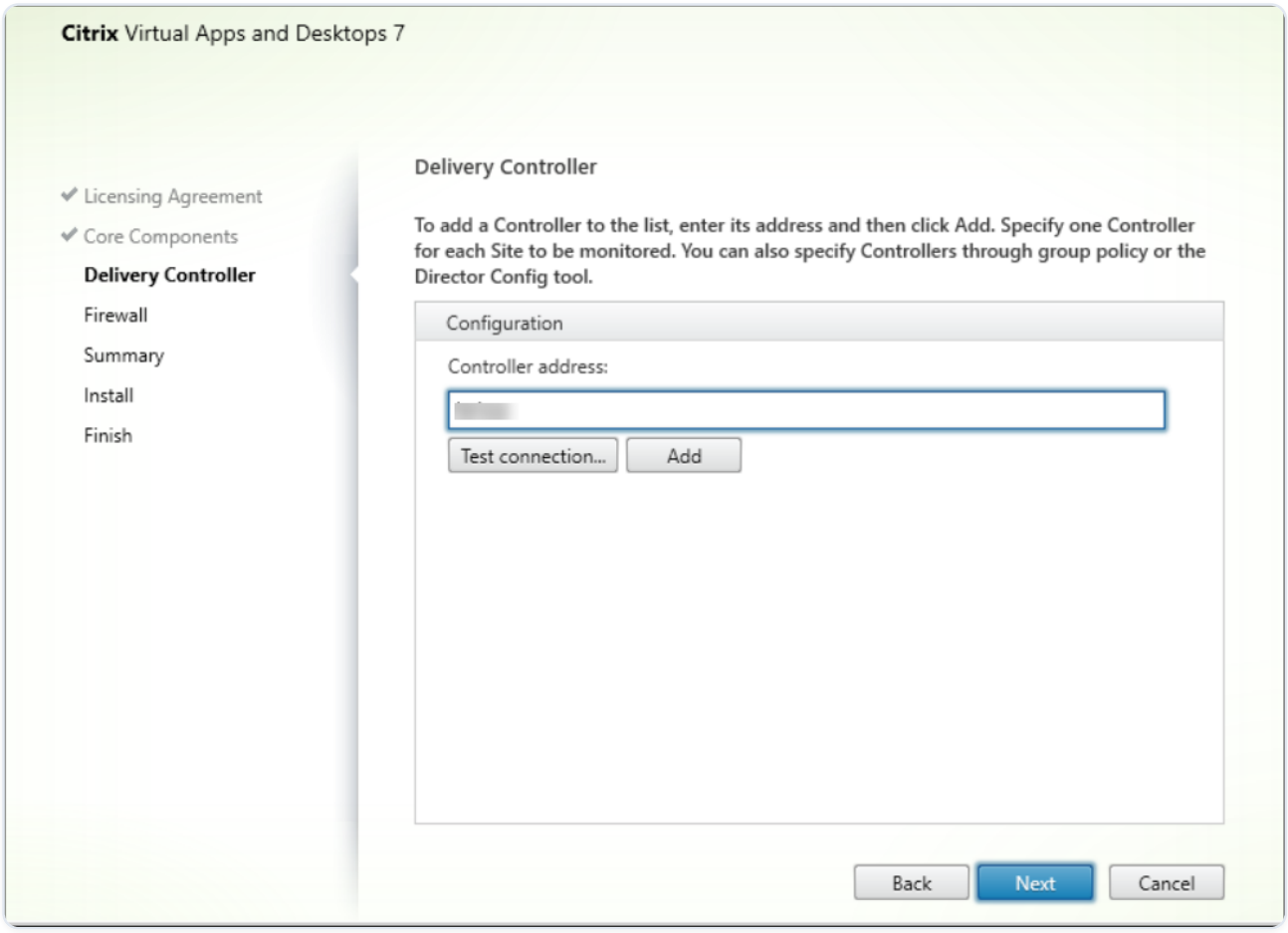
```
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

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 o endereço do servidor, e o Director se comunica com o Controller local por padrão. Para instalar o Director em um servidor dedicado que está 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 Controllers, Director e outros componentes principais estão instalados. Caso contrário, os sites podem não ser exibidos corretamente no Director.

> **Importante:**
>
> Para proteger a segurança de nomes de usuário e senhas enviados em texto simples pela rede, permita conexões do Director usando apenas HTTPS, e não HTTP. Certas ferramentas são capazes de ler nomes de usuário e senhas em texto simples em pacotes de rede HTTP (não criptografados), o que pode criar um risco potencial de segurança para os usuários.

Configurar permissões

Para fazer logon no Director, os administradores com permissões para o Director devem ser usuários de domínio do Active Directory e devem ter os seguintes direitos:

- Direitos de leitura em todas as florestas do Active Directory a serem pesquisadas (consulte Configuração avançada).
- Funções de Administrador Delegado configuradas (consulte administração delegada e Director).
- Para sombrear usuários, os administradores devem ser configurados usando uma política de grupo da Microsoft para Assistência Remota do Windows. Além disso:
  - Ao instalar VDAs, certifique-se de que o recurso Assistência Remota do Windows esteja habilitado em todos os dispositivos de usuário (selecionado por padrão).
  - Ao instalar o Director em um servidor, certifique-se de que a Assistência Remota do Windows esteja instalada (selecionada por padrão). No entanto, ela é desabilitada no servidor por padrão. O recurso não precisa ser habilitado para que o Director forneça assistência aos usuários finais. A Citrix recomenda deixar o recurso desabilitado para melhorar a segurança no servidor.

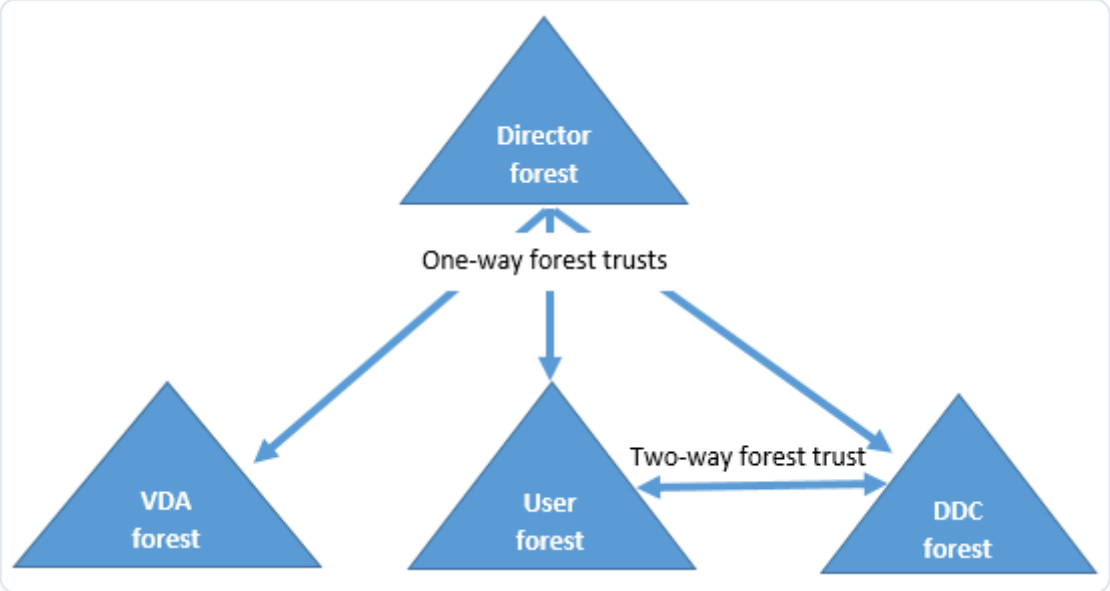
- Para permitir que os administradores iniciem a Assistência Remota do Windows, conceda a eles as permissões necessárias usando as configurações apropriadas da Política de Grupo da Microsoft para Assistência Remota. Para obter informações, consulte CTX127388: Como Habilitar a Assistência Remota para o Desktop Director.

Configuração avançada

O Director pode suportar ambientes multiflorestas que abrangem uma configuração de floresta onde usuários, Delivery Controllers (DCs), VDAs e Directors estão localizados em florestas diferentes. Isso requer a configuração adequada de relações de confiança entre as florestas e as configurações.

Configuração recomendada em um ambiente multifloresta

A configuração recomendada exige a criação de relações de confiança de floresta de saída e de entrada entre as florestas com autenticação em todo o domínio.



A relação de confiança do Director permite solucionar problemas em sessões de usuário, VDAs e Delivery Controllers localizados em florestas diferentes.

A configuração avançada necessária para o Director suportar 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 procurar usuários e para pesquisar mais informações de usuário e máquina. Por padrão, o Director pesquisa o domínio ou floresta em que:

- A conta do administrador é membro.
- O servidor web do Director é membro (se diferente).

O Director tenta realizar pesquisas no nível da floresta usando o catálogo global do Active Directory. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

A pesquisa ou consulta de dados de outro domínio ou floresta do Active Directory exige que você defina explicitamente os domínios ou florestas a serem pesquisados. Configure a seguinte configuração de Aplicativos para o site do Director no Gerenciador do IIS:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Os atributos de valor user e server representam os domínios do usuário do Director (o administrador) e do servidor do Director, respectivamente.

Para habilitar pesquisas de um domínio ou floresta extra, adicione o nome do domínio à lista, conforme mostrado neste exemplo:

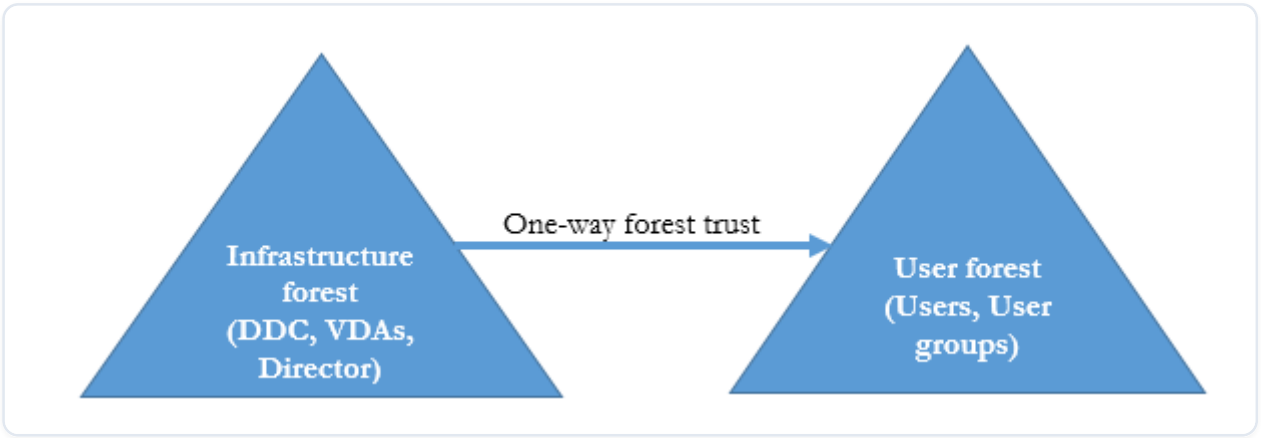
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

Para cada domínio na lista, o Director tenta realizar pesquisas no nível da floresta. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

Configuração de grupo local de domínio

A maioria dos Provedores de Serviços Citrix (CSPs) tem configurações de ambiente semelhantes, consistindo em VDAs, DCs e Director na floresta de Infraestrutura. Os registros de usuários ou grupos de usuários pertencem à floresta do Cliente. Existe uma 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 multifloresta como esta e monitorar as sessões de usuários configurados usando grupos locais de domínio.

1. Adicione as seguintes configurações de Aplicativos ao site do Director no Gerenciador do IIS:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> são nomes das florestas nas quais o grupo local de domínio existe.

2. Atribua o grupo local de domínio aos grupos de entrega no Citrix 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. Esta informação é visualizada por todos os administradores que têm acesso ao recurso Gerenciador de Atividades no Director. Para funções de Administrador Delegado, isso inclui Administrador Completo, Administrador de grupo de entrega e Administrador de Help Desk.

Para proteger a privacidade dos usuários e dos aplicativos que eles estão executando, você pode desabilitar a guia **Aplicativos** para listar os aplicativos em execução.

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

1. No VDA, modifique a chave do registro em `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`. Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, portanto, não são exibidas no Gerenciador de Atividades.
2. No servidor com o Director instalado, modifique a configuração que controla a visibilidade dos aplicativos em execução. Por padrão, o valor é "true", o que permite a visibilidade dos aplicativos em execução na guia Aplicativos. Altere o valor para "false", o que desabilita a

visibilidade. Esta opção afeta apenas o Gerenciador de Atividades no Director, não o VDA. Modifique o valor da seguinte configuração: UI.TaskManager.EnableApplications = false

Importante:

Para desabilitar a visualização de aplicativos em execução, faça ambas as alterações para garantir que os dados não sejam exibidos no Gerenciador de Atividades.

Configurar autenticação de cartão inteligente PIV

Este artigo lista a configuração necessária no Servidor Director e no Active Directory para habilitar o recurso de autenticação de cartão inteligente.

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:

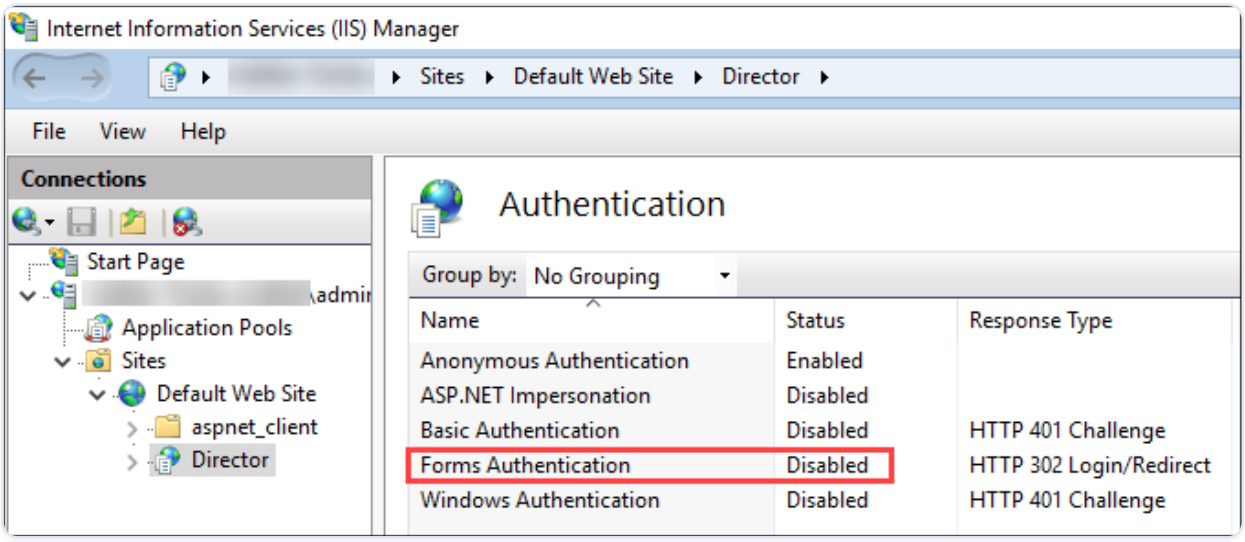
1. Instale e habilite a Autenticação de Mapeamento de Certificado de Cliente. Siga as instruções de **Autenticação de mapeamento de certificado de cliente usando o Active Directory** no documento da Microsoft, Autenticação de Mapeamento de Certificado de Cliente.
2. Desabilite a Autenticação de Formulários 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.**



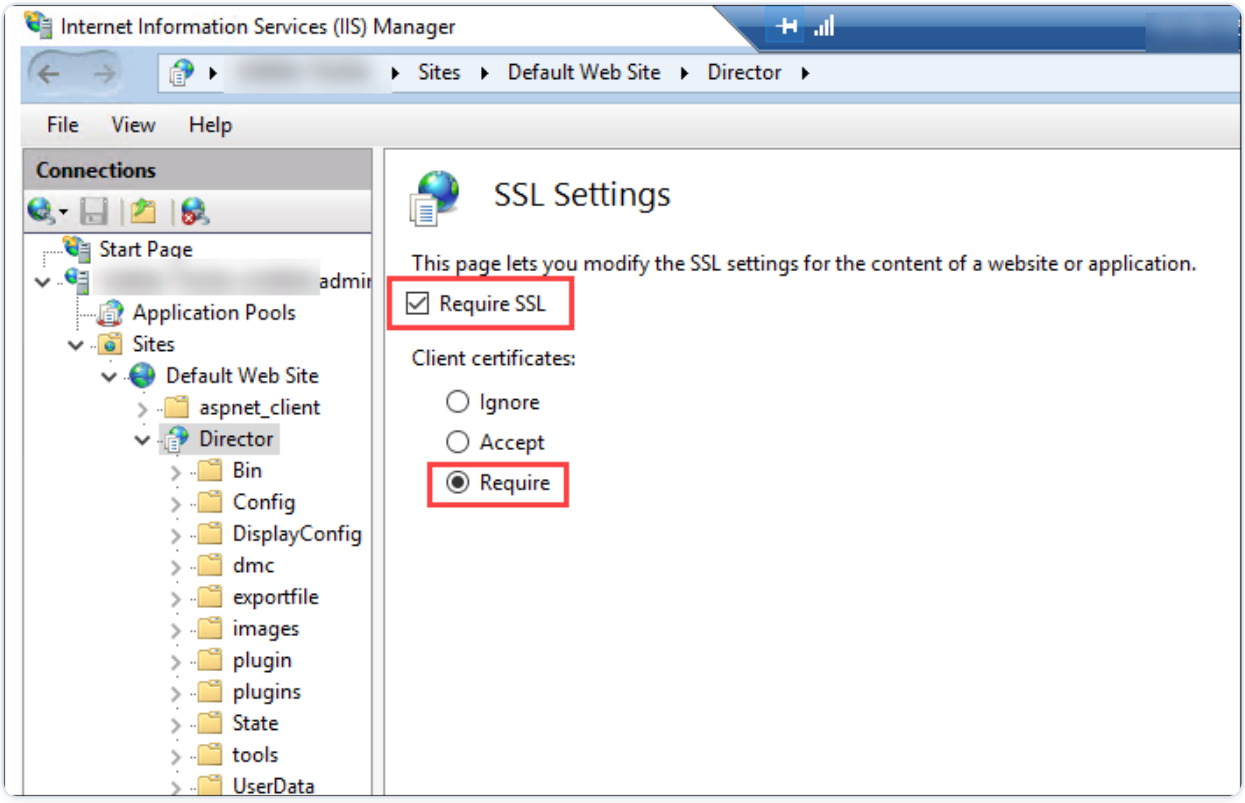
3. Configure a URL do Director para o protocolo https mais seguro (em vez de HTTP) para autenticação de certificado de cliente.

   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;

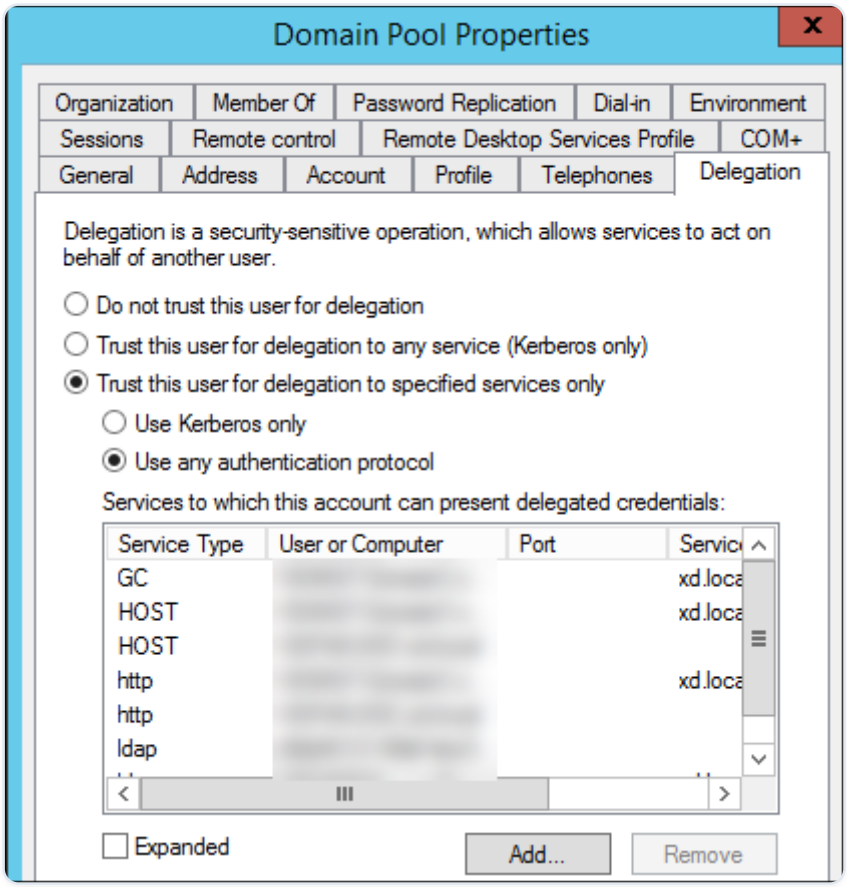
&lt;/defaultDocument&gt;
```

Configuração do Active Directory

Por padrão, o aplicativo Director é executado com a propriedade de identidade do **Pool de Aplicativos**. A autenticação por cartão inteligente requer delegação para a qual a identidade do aplicativo Director deve ter privilégios de Trusted Computing Base (TCB) no host do serviço.

A Citrix recomenda que você crie uma conta de serviço separada para a identidade do 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.

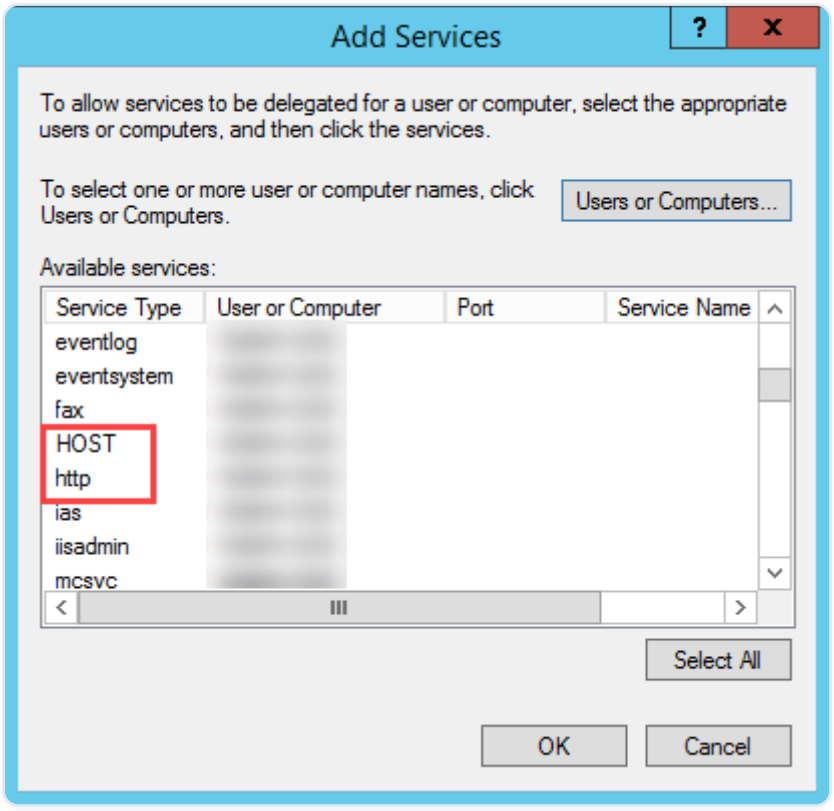


Configure os seguintes serviços para esta conta:

- 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 **Director** e **Active Directory**.

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 Instalando o Módulo OpenSC PKCS#11 no Firefox, Passo a Passo. Para obter informações sobre o uso do recurso de autenticação de cartão inteligente no Director, consulte a seção Usar o Director com autenticação de cartão inteligente baseada em PIV 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 fornece retenção histórica e relatórios de tendências. Com a retenção histórica de dados em comparação com a avaliação em tempo real, você pode criar relatórios de tendências, incluindo tendências de capacidade e integridade.

Depois de habilitar esse recurso no Director, os relatórios 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 visualização Tendências, os dados de logon de conexão HDX não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.

Para habilitar a análise de rede, você deve instalar e configurar o Citrix ADM no Director. O Director requer o Citrix ADM Versão 11.1 Build 49.16 ou posterior. O MAS é um appliance virtual que é executado no Citrix 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 recomendável 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 incorporadas também determinam como os administradores usam o Director:

FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO DIRECTOR
Administrador Completo	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o modo de manutenção e exportar dados de tendências.
Administrador de grupo de entrega	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o

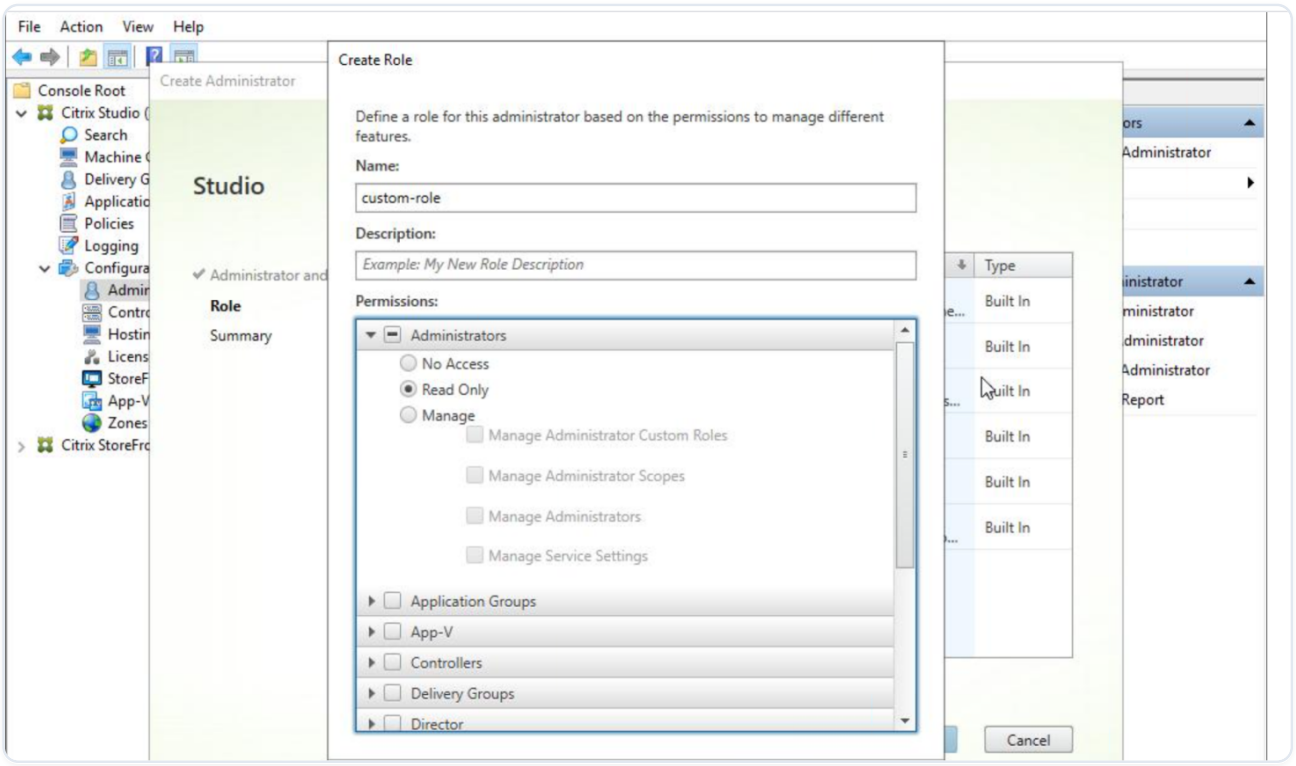
FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO DIRECTOR
	modo de manutenção e exportar dados de tendências.
Administrador Somente Leitura	Pode acessar todas as visualizações e ver todos os objetos em escopos especificados e informações globais. Pode baixar relatórios de canais HDX™ e exportar dados de Tendências usando a opção Exportar na visualização Tendências. Não pode executar outros comandos 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 acompanhar 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 Painel, Tendências, Alertas ou Filtros. Não pode usar opções de controle de energia para máquinas OS de várias sessões.
Administrador de catálogo de máquinas	Pode acessar apenas a página Detalhes da Máquina (pesquisa baseada em máquina).
Administrador de Host	Sem acesso. Este administrador não é 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 incorporada para que este administrador não possa encerrar sessões.

Se você criar uma função personalizada com permissões do Director, também deverá conceder a essa função outras permissões genéricas:

- Permissão do Delivery Controller™ para fazer logon no Director - pelo menos acesso somente leitura no nó Administrador
- Permissões para grupos de entrega para visualizar os dados relacionados a esses grupos de entrega no Director - pelo menos acesso somente leitura

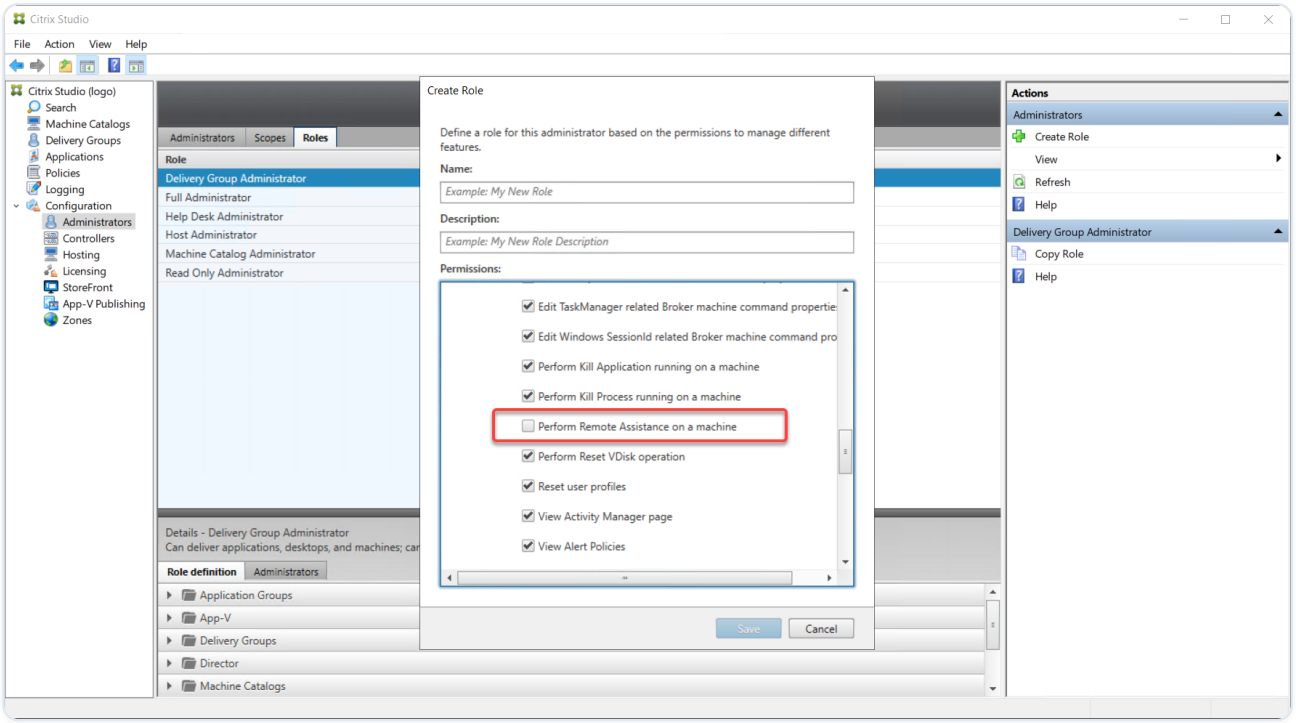


Alternativamente, você pode criar uma função personalizada copiando uma função existente e incluindo permissões extras para diferentes visualizações. Por exemplo, você pode copiar a função de Help Desk e incluir permissões para visualizar as páginas de Painel ou Filtros.

Selecione as permissões do Director para a função personalizada, que incluem:

- Executar Encerrar Aplicativo em execução em uma máquina
- Executar Encerrar Processo em execução em uma máquina
- Executar Assistência Remota em uma máquina
- Redefinir perfis de usuário
- Visualizar página de Detalhes do Cliente
- Visualizar página do Painel
- Visualizar página de Filtros
- Visualizar página de Detalhes da Máquina
- Visualizar página de Tendências
- Visualizar página de Detalhes do Usuário

Neste exemplo, o Shadowing (Executar Assistência Remota em uma máquina) está desativado.



Uma permissão pode ter dependências de outras permissões para se tornar aplicável na interface do usuário. Por exemplo, selecionar a permissão **Executar Encerrar Aplicativo em execução em uma máquina** habilita a funcionalidade **Encerrar Aplicativo** apenas nos painéis para os quais a função tem permissão. Você pode selecionar as seguintes permissões de painel:

- Visualizar página de Filtros
- 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 dos grupos de entrega:

- Ativar/desativar o modo de manutenção de uma máquina usando a associação ao grupo de entrega.
- Executar operações de energia em máquinas Windows Desktop usando a associação ao grupo de entrega.
- Executar gerenciamento de sessão em máquinas usando a associação ao grupo de entrega.

Implantação segura do Director

Este artigo destaca áreas que podem ter um impacto na segurança do sistema ao implantar e configurar o Director.

Configurar o Microsoft Internet Information Services (IIS)

Você pode configurar o Director com uma configuração restrita do IIS.

Limites de reciclagem do Pool de Aplicativos

Você pode definir os seguintes limites de reciclagem do Pool de Aplicativos:

- Limite de Memória Virtual: 4.294.967.295
- Limite de Memória Privada: O tamanho da memória física do servidor StoreFront™
- Limite de Solicitações: 4.000.000.000

Extensões de nome de arquivo

Você pode desabilitar extensões de nome de arquivo não listadas.

O Director requer estas extensões de nome de arquivo na Filtragem de Solicitações:

- .ASPX
- .CSS
- .html
- .js
- .png
- .svc
- extensão .gif
- extensão .json
- .woff
- .woff2
- .TTF

O Director requer os seguintes verbos HTTP no Filtro 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 um comportamento normal de instalação quando os pools de aplicativos são criados.

Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Director e são desativados automaticamente.

Comunicações do Director

Em um ambiente de produção, use os protocolos de segurança do Protocolo de Internet (IPsec) ou HTTPS para proteger os dados que trafegam entre o Director e seus servidores.

O IPsec é um conjunto de extensões padrão para o Protocolo de Internet que fornece comunicações autenticadas e criptografadas com integridade de dados e proteção contra repetição. Como o IPsec é um conjunto de protocolos de camada de rede, protocolos de nível superior podem usá-lo sem modificação. O HTTPS usa os protocolos Transport Layer Security (TLS) para fornecer criptografia de dados forte.

Observação:

- A Citrix® recomenda fortemente que você restrinja o acesso ao console do Director dentro da rede intranet.
- A Citrix recomenda fortemente que você não habilite conexões não seguras ao Director em um ambiente de produção.
- Comunicações seguras do Director exigem configuração para cada conexão separadamente.
- O protocolo SSL não é recomendado. Use o protocolo TLS, que é mais seguro, em vez disso.
- Proteja suas comunicações com o Citrix ADC usando TLS, não IPsec.

Para proteger as comunicações entre o Director e os servidores Citrix Virtual Apps and Desktops (para monitoramento e relatórios), consulte Segurança de Acesso a Dados.

Para proteger as comunicações entre o Director e o Citrix ADC (para Citrix Insight), consulte Configurar análise de rede.

Para proteger as comunicações entre o Director e o servidor de licenças, consulte Proteger o Console de Administração de Licenças.

Separação de segurança do Director

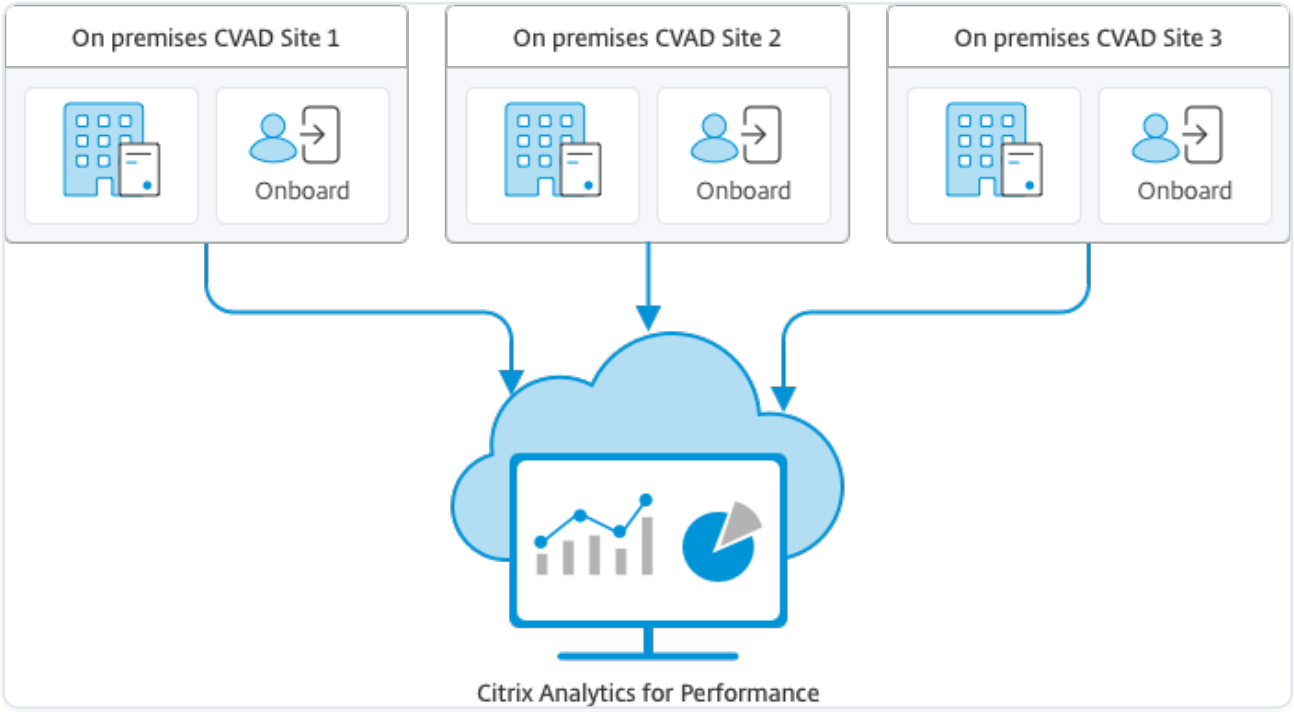
Você pode implantar quaisquer aplicativos web no mesmo domínio web (nome de domínio e porta) que o Director. No entanto, quaisquer riscos de segurança nesses aplicativos web podem potencialmente reduzir a segurança da sua implantação do Director. Onde um maior grau de separação de segurança é necessário, a Citrix recomenda que você implante o Director em um domínio web separado.

Configurando sites locais com Citrix Analytics for Performance™

O Citrix Analytics for Performance (Performance Analytics) é a solução abrangente de monitoramento de desempenho do Citrix Analytics Cloud Service. O Performance Analytics fornece insights e análises avançadas construídas sobre métricas de desempenho. O Performance Analytics ajuda você a monitorar e visualizar o uso e as métricas de desempenho de um ou mais sites do Citrix Virtual Apps and Desktops™ em sua organização.

Para obter mais informações sobre o Performance Analytics, consulte o artigo do Performance Analytics.

Você pode enviar dados de desempenho do seu site para o Citrix Analytics for Performance no Citrix Cloud™ para aproveitar seus recursos avançados de análise de desempenho. Para visualizar e usar o Performance Analytics, você deve primeiro configurar seus sites locais com o Citrix Analytics for Performance na guia **Analytics** no **Director**.



O Performance Analytics acessa os dados de forma segura e nenhum dado é transferido do Citrix Cloud para o ambiente local.

Pré-requisitos

Para configurar o Citrix Analytics for Performance a partir do Director, nenhum novo componente precisa ser instalado. Certifique-se de que os seguintes requisitos sejam atendidos:

- Seu Delivery Controller e Director estão na versão 1912 CU2 ou posterior. Para obter mais informações, consulte Matriz de compatibilidade de recursos.

> **Observação:**
>
> - A configuração do seu site local com o Citrix Analytics for Performance a partir do Director pode falhar se o Delivery Controller estiver executando uma versão do Microsoft .NET Framework anterior à 4.8. Como solução alternativa, atualize o .NET Framework em seu Delivery Controller para a versão 4.8. LCM-9255.
> - Ao configurar seu site local executando o Citrix Virtual Apps and Desktops versão 2012 com o Citrix Analytics for Performance a partir do Director, a configuração pode falhar

> após algumas horas ou após uma reinicialização do Serviço de Monitoramento Citrix no Delivery Controller. A guia Analytics exibe um status Não Conectado neste caso. Como solução alternativa, crie uma pasta Encryption no registro 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 nas quais o Director está instalado. Especificamente, garanta a acessibilidade aos seguintes URLs:
  - Registro de Chave Citrix: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Caso os Delivery Controllers e as máquinas Director estejam em uma intranet e o acesso à internet de saída seja feito por meio de um servidor proxy, certifique-se do seguinte:
- O servidor proxy deve permitir a lista de URLs anterior.
- Adicione a seguinte configuração nos arquivos web.config do Director e citrix.monitor.exe.config. Certifique-se de adicionar esta configuração dentro das tags **configuration**:

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

- O web.config do Director está localizado em `C:\inetpub\wwwroot\Director\web.config` na máquina onde o Director está instalado.
- O citrix.monitor.exe.config está localizado em `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` na máquina onde o Delivery Controller está instalado.

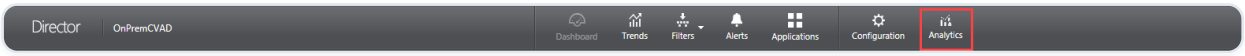
Essa configuração é fornecida pela Microsoft no IIS. Para obter mais informações, consulte `https://docs.microsoft.com/pt-br/dotnet/framework/network-programming/proxy-configuration`. O campo **defaultproxy** no arquivo de configuração controla o acesso de saída do Director e do Monitor Service. A configuração e a comunicação com o Performance Analytics exigem que o campo **defaultproxy** seja definido como **true**. É possível que as políticas em vigor definam 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.

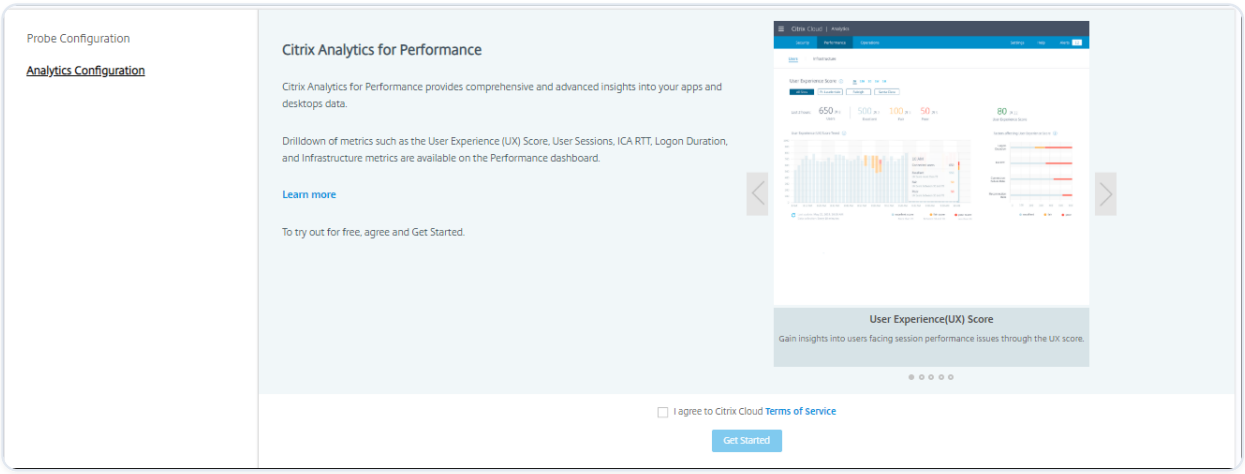
Etapas de configuração

Depois de verificar os pré-requisitos, faça o seguinte:

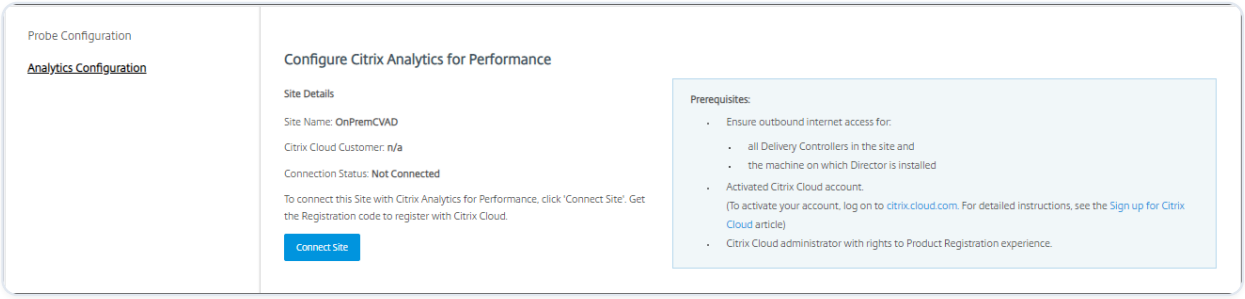
1. Faça logon no Director como administrador completo e selecione o site que você deseja configurar com o Performance Analytics.
2. Clique na guia **Analytics**. A página **Configuração** é exibida.



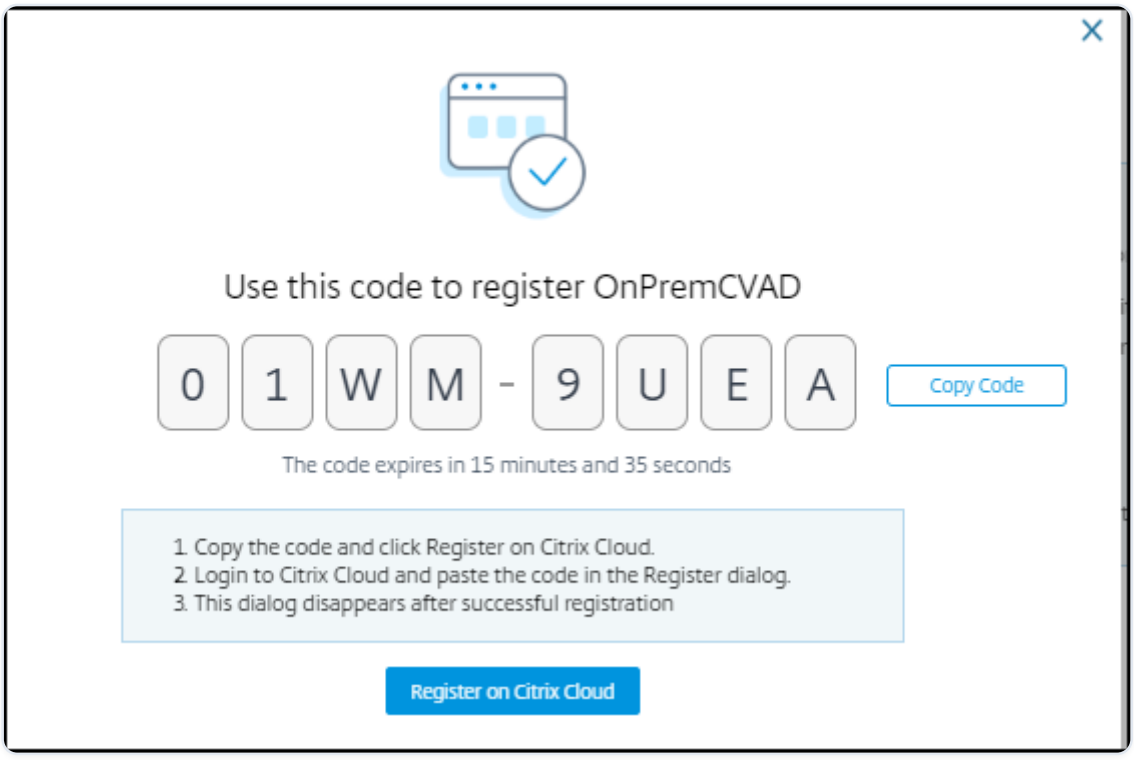
3. Revise as etapas, selecione os termos de serviço e clique em **Começar**.



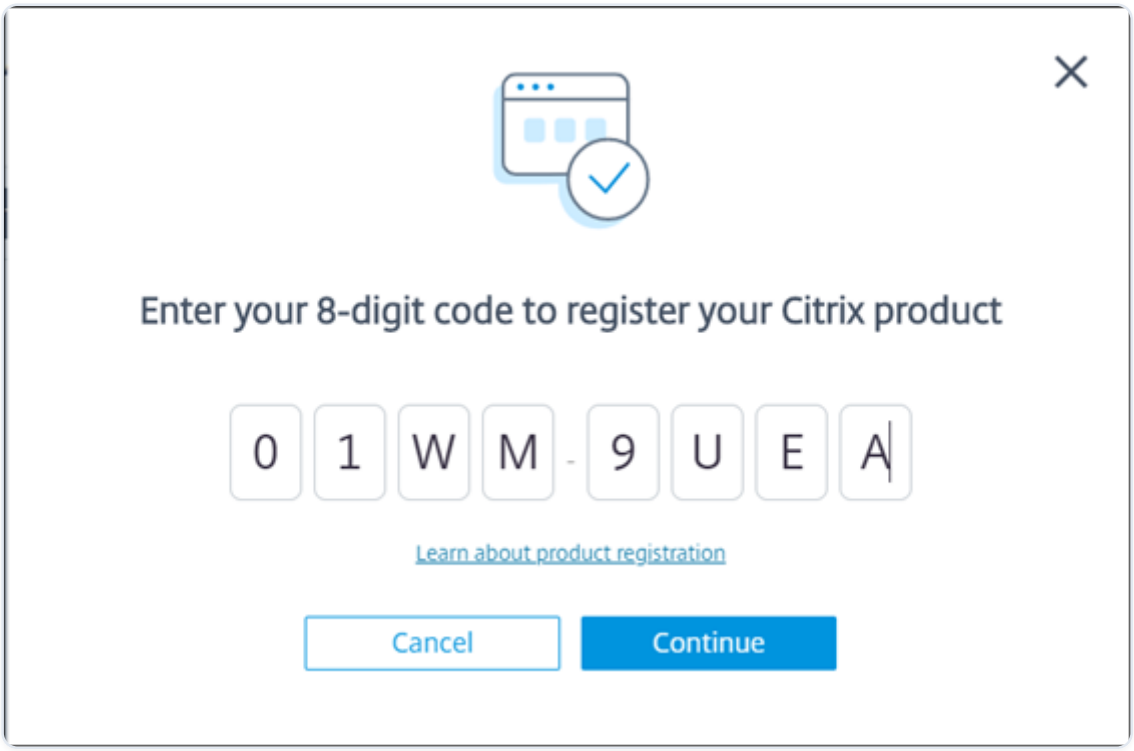
4. Revise os pré-requisitos e certifique-se de que eles sejam atendidos. Revise os Detalhes do site.
5. Clique em **Conectar Site** para iniciar o processo de configuração.



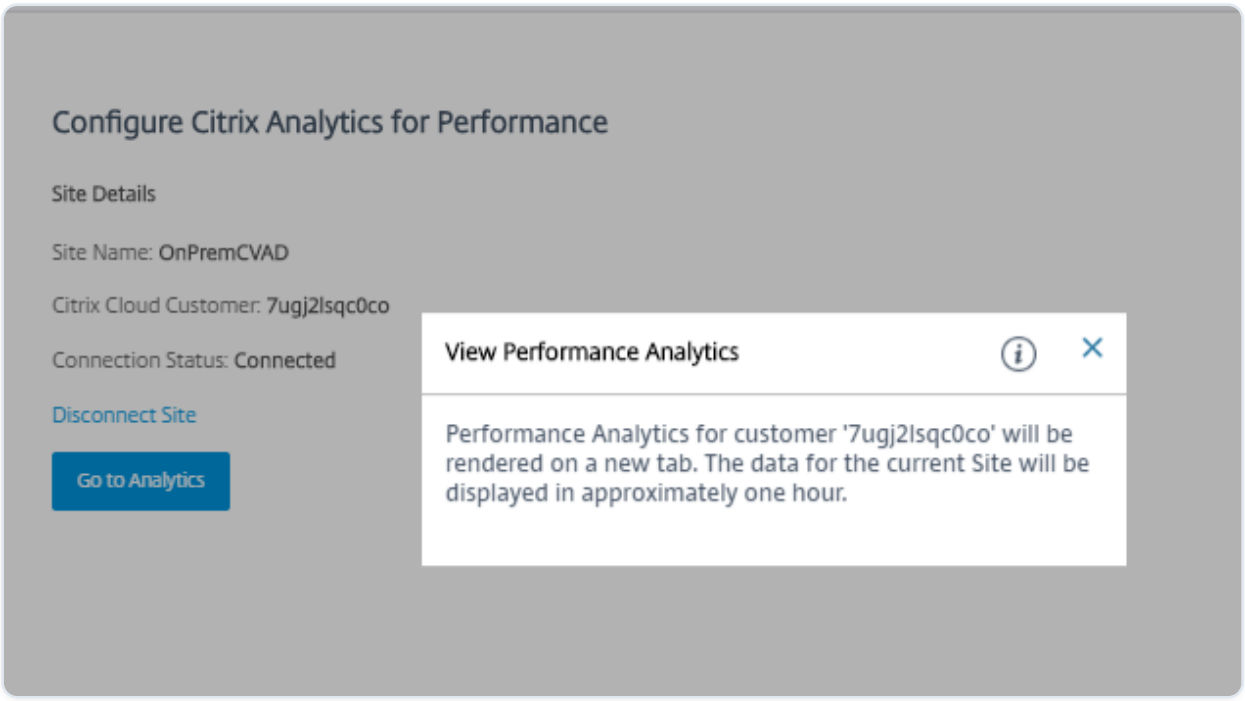
6. Um código de registro exclusivo de 8 dígitos é gerado para ser usado para registrar este site no Citrix Cloud.



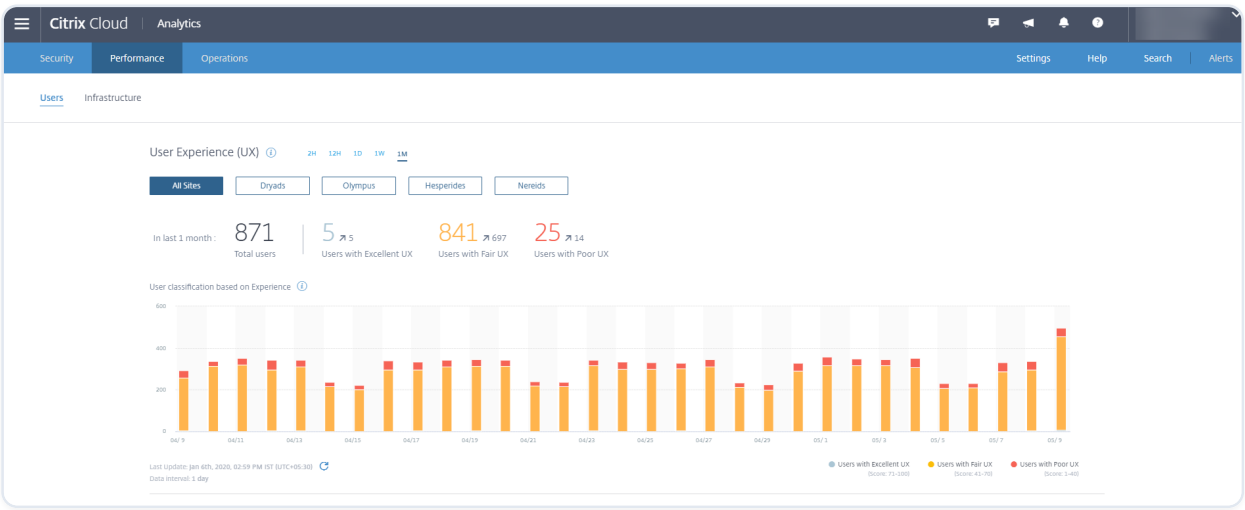
7. Clique em **Copiar Código** para copiar o código e, em seguida, clique em **Registrar no Citrix Cloud**.
8. Você será redirecionado para a URL de Registro no Citrix Cloud. Faça login com suas credenciais do Citrix Cloud e selecione seu cliente.
9. Cole o código de registro copiado na página Registros de Produto no Citrix Cloud. Clique em **Continuar** para registrar. Revise os detalhes do registro e clique em **Registrar**.



10. Seu site local se registra no Citrix Cloud. Agora, no **Director**, clique em **Ir para Análise** na guia **Análise**.



11. A Análise de Desempenho é aberta 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.

12. 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.

13. Para desconectar seu site do Citrix Cloud, clique em **Desconectar Site**. Esta opção exclui a configuração existente.

Observações:

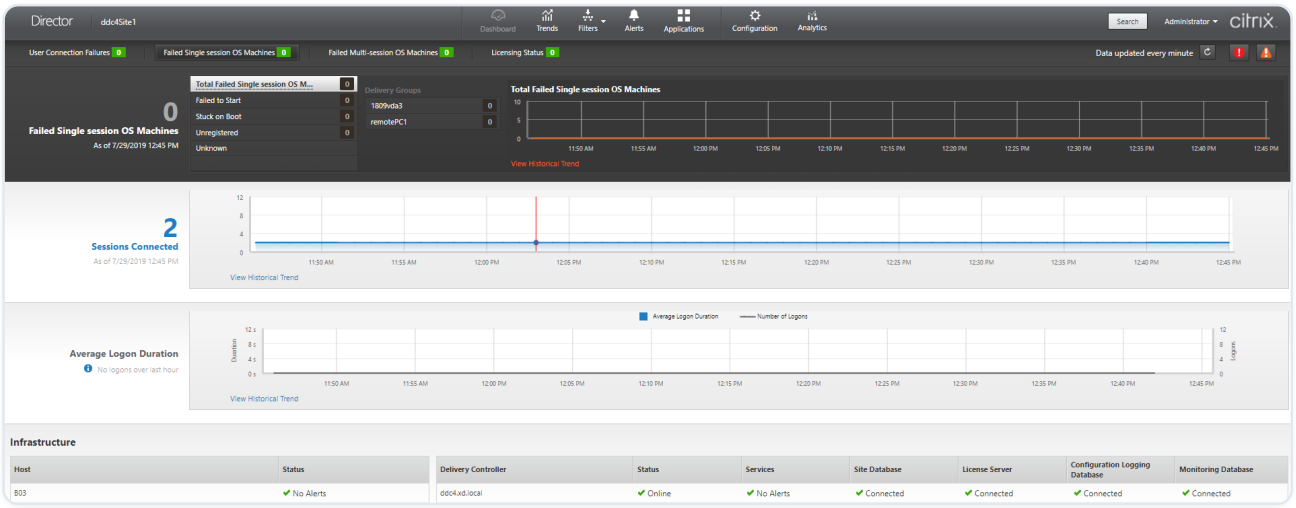
Na primeira vez que você configura um site, os eventos do site podem levar algum tempo (aproximadamente uma hora) para serem processados, causando um atraso na exibição das métricas no painel do Performance Analytics. Depois disso, os eventos são atualizados em intervalos regulares.

Após a desconexão, a transmissão de dados da conta antiga continua por algum tempo até que os eventos da nova conta sejam transmitidos. Por aproximadamente uma hora após a interrupção da transmissão de dados, as análises relacionadas à conta antiga permanecem exibidas no Painel do Performance Analytics.

Após a expiração do direito ao serviço Citrix Analytics, leva até um dia para parar de enviar as métricas do site para o Performance Analytics.

Análise do Site

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.

Nota:

> Dependendo da licença da sua organização e dos seus privilégios de Administrador, algumas opções ou recursos podem não estar disponíveis.

Painéis no Painel do Director

Falhas de Conexão do Usuário

Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para visualizar métricas para esse tipo de falha. Na tabela adjacente, esse número é detalhado por grupos de entrega. As falhas de conexão incluem falhas causadas pelo atingimento dos limites do aplicativo. Para obter mais informações sobre limites de aplicativos, consulte Aplicativos.

Máquinas OS de sessão única com falha ou Máquinas OS de várias sessões com falha

Total de falhas nos últimos 60 minutos detalhadas por grupos de entrega. Falhas detalhadas por tipo, incluindo falha ao iniciar, travado na inicialização e não registrado. Para máquinas com SO de múltiplas sessões, as falhas também incluem máquinas atingindo carga máxima.

Status de Licenciamento

Os alertas do Servidor de Licenças exibem alertas enviados pelo Servidor de Licenças e as ações necessárias para resolver os alertas. Requer Servidor de Licenças Versão 11.12.1 ou posterior. Os alertas do Delivery Controller exibem os detalhes do estado de licenciamento conforme visto pelo Controller e são enviados pelo Controller. Requer Controller para XenApp 7.6 ou XenDesktop 7.6 ou posterior. Você pode definir o limite para alertas no Studio. O status de licenciamento exibido em **Delivery Controllers** > **Detalhes** > **Edições do Produto** > **PLT** indica **Premium** e não **Platinum**.

Estado de Carência

O Director exibe um dos seguintes estados de carência. Esta informação é obtida do Delivery Controller.

1. **Não Ativo:** Não está em nenhum tipo de modo de cache de licença. Limites normais de licenciamento se aplicam.
2. **Carência de Emergência:** Entra em vigor quando o servidor de licenças está inacessível ou as informações da licença não podem ser obtidas durante a intermediação de uma conexão. Os usuários não são afetados. Os erros exibidos no Director não podem ser ignorados até que o servidor de licenças esteja acessível.

3. **Carência Expirada:** O modo de cache de licença de emergência expirou.

Para obter mais informações, consulte Excesso de licença e Modo de intermitência de licença.

Sessões Conectadas

Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.

Duração Média do Logon

Dados de logon dos últimos 60 minutos. O número grande à esquerda é a duração média do logon ao longo da hora. Os dados de logon para VDAs anteriores ao XenDesktop 7.0 não estão incluídos nesta média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Infraestrutura

Lista a infraestrutura do seu site - hosts e Controllers. Para infraestrutura do Citrix Hypervisor 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 Citrix Hypervisor.

> **Nota:**
>
> 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 Dashboard, 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 entre 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 sessão de antes dos últimos 60 minutos). Para visualizar esta

AÇÃO	DESCRIÇÃO
	informação, clique em **Ver tendências históricas**.

Nota:

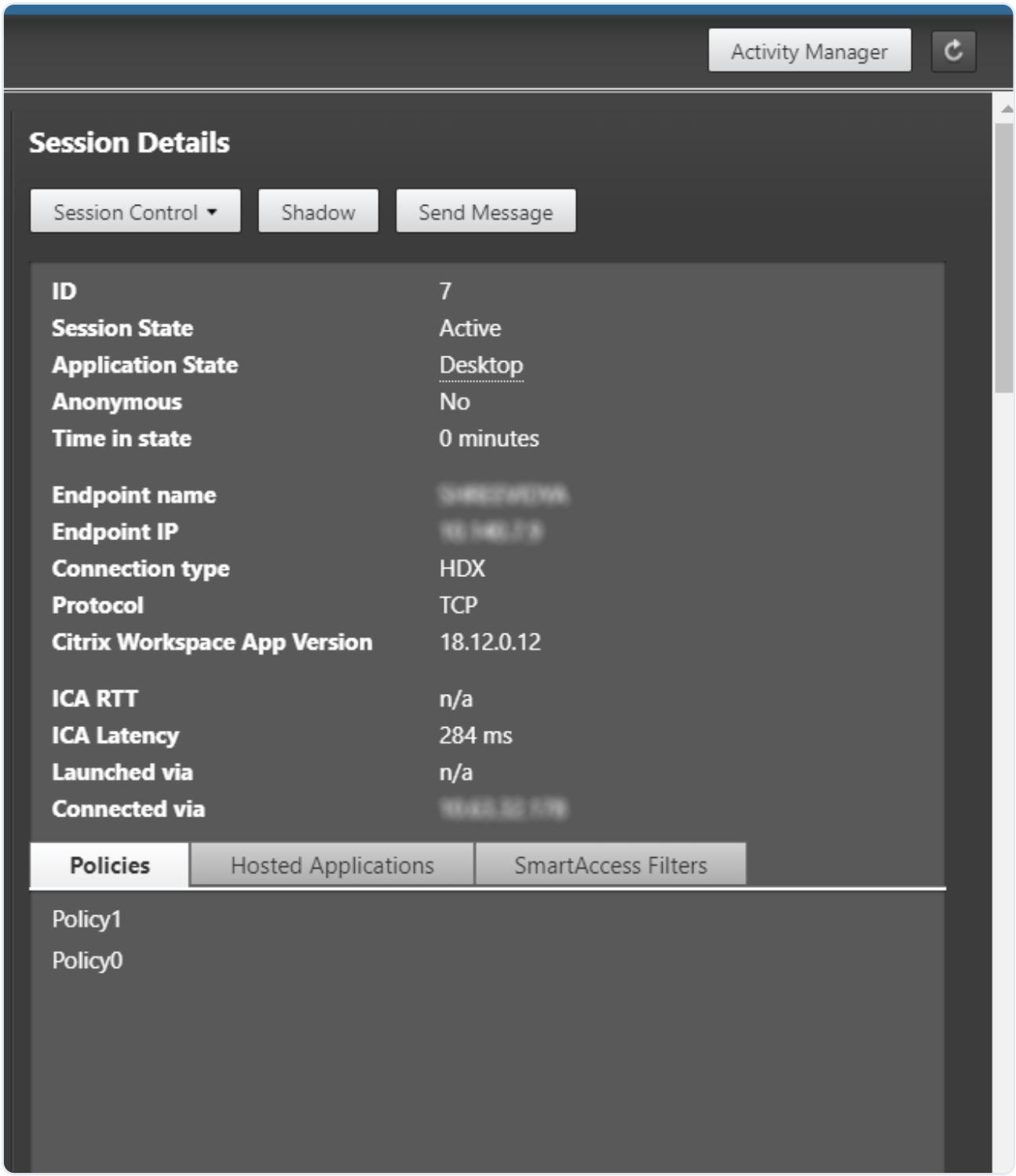
Se o dispositivo do usuário estiver executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7, ou um VDA Linux, o Director não poderá exibir informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem informando que as informações não estão disponíveis.

Limitação das Regras de Atribuição de Desktop: O Citrix Studio permite a atribuição de múltiplas 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 oferece suporte a DARs e exibe o desktop atribuído usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear um desktop específico para uma máquina no 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 de sessão

Visualize o protocolo de transporte em uso para o tipo de conexão HDX da sessão atual no painel **Detalhes da Sessão**. Esta informação está disponível para sessões iniciadas em VDAs Versão 7.13 ou posterior.



- Para o tipo de conexão **HDX™**,
  - O Protocolo é exibido como **UDP**, se o EDT for usado para a conexão HDX.
  - O Protocolo é exibido como **TCP**, se o TCP for usado para a conexão HDX.
- Para o tipo de conexão **RDP**, o Protocolo é exibido como **n/a**.

Quando o transporte adaptativo é configurado, o protocolo de transporte da sessão alterna dinamicamente entre EDT (sobre UDP) e TCP, com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ela retornará ao protocolo TCP.

Para obter mais informações sobre a configuração de transporte adaptável, consulte Transporte Adaptável.

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 que você seleciona. Se você alterar os critérios de filtro, clique em **Aplicar** antes de clicar em **Exportar**.

> **Nota:**
>
> A exportação de uma grande quantidade de dados causa um aumento significativo no consumo de memória e CPU no servidor Director, no Delivery Controller e nos servidores SQL. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados é definido para limites padrão para alcançar o desempenho ideal de exportação.

Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos para os critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados além dos limites padrão no número de linhas ou registros na tabela. O número padrão de registros suportados é definido com base no formato do relatório.

Você pode alterar o limite padrão configurando as Configurações do Aplicativo 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 Site Padrão.
3. Clique duas vezes em **Configurações do Aplicativo**.
4. Edite ou adicione uma configuração para os campos UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit ou UI.ExportCsvDrilldownLimit conforme necessário.

Adicionar esses valores de campo em Configurações do Aplicativo 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 de Monitoramento.

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 em** 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 **Configurações do Aplicativo**.
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 de Monitoramento ou no servidor SQL.

Para aumentar a duração do tempo limite do Serviço de Monitoramento, 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 de Exportação ou Visualização simultâneas, no entanto, isso pode afetar o desempenho do Director e não é suportado:

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Default website.
3. Clique duas vezes em **Application Settings**.
4. Edite o valor **UI.ConcurrentExportLimit**.

- **Espaço em disco insuficiente no Director**

Cada operação de Exportação requer um máximo de 2 GB de espaço em disco rígido na pasta Temp do Windows. Tente exportar novamente depois de liberar espaço ou adicionar mais espaço em disco rígido no servidor Director.

Hotfixes do Monitor

Para visualizar os hotfixes instalados em um VDA de máquina específico (físico ou VM), escolha a exibição **Detalhes da Máquina**.

Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas que você seleciona no Director, use as opções de Controle de Energia. Essas opções estão disponíveis para máquinas de SO de sessão única, mas podem não estar disponíveis para máquinas de SO de várias sessões.

Nota:

Essa 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.

COMANDO	FUNÇÃO
Desligar	Executa um desligamento ordenado (suave) da VM. Todos os processos em execução são interrompidos individualmente.
Forçar Desligamento	Desliga a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico. 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 são desconectados. Para usuários que não se desconectam, envie uma mensagem informando que as máquinas serão desligadas em um determinado horário e use os controles de energia para forçar o desligamento das máquinas.

1. Selecione a máquina, como na exibição Detalhes do Usuário, ou um grupo de máquinas na exibição Filtros.
2. Selecione **Modo de Manutenção** e ative a opção.

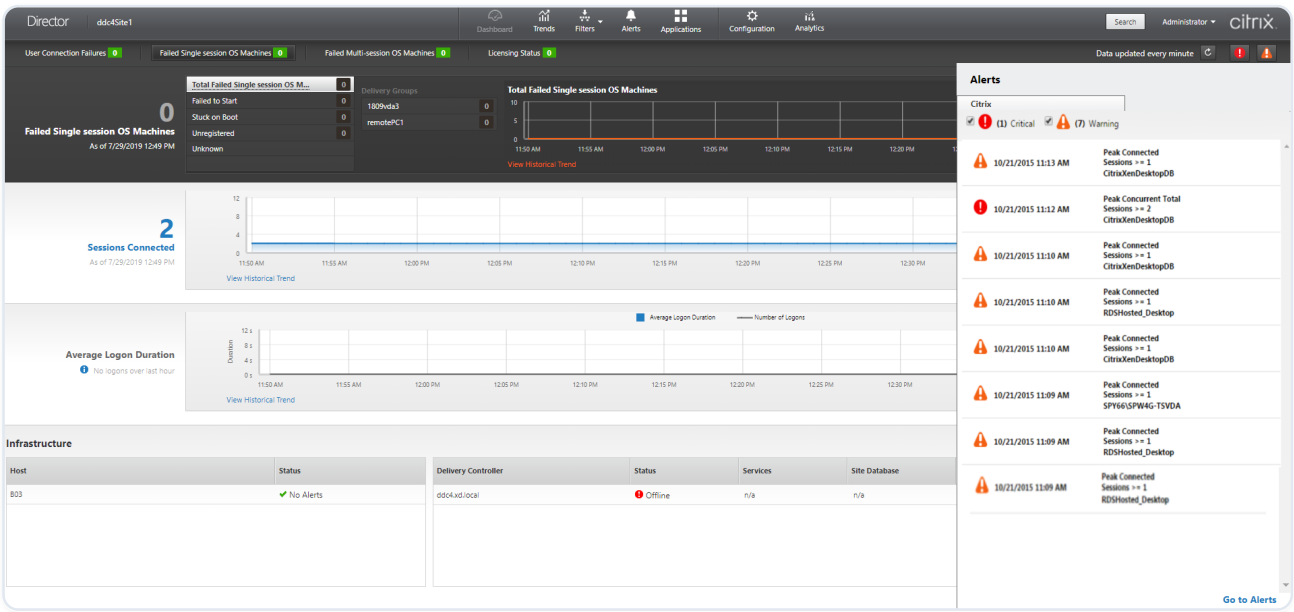
Se um usuário tentar se conectar a um desktop atribuído enquanto ele estiver no modo de manutenção, uma mensagem aparecerá indicando que o desktop está indisponível. Nenhuma nova conexão pode ser feita até que você desabilite o modo de manutenção.

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 dos aplicativos de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. Ela mostra métricas como os resultados da sonda, 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

Os alertas são exibidos no Director no painel e em outras visualizações de alto nível com símbolos de alerta de aviso e críticos. Os alertas estão disponíveis para sites com licença **Premium**. Os alertas são atualizados automaticamente a cada minuto; você também pode atualizar os alertas sob demanda.

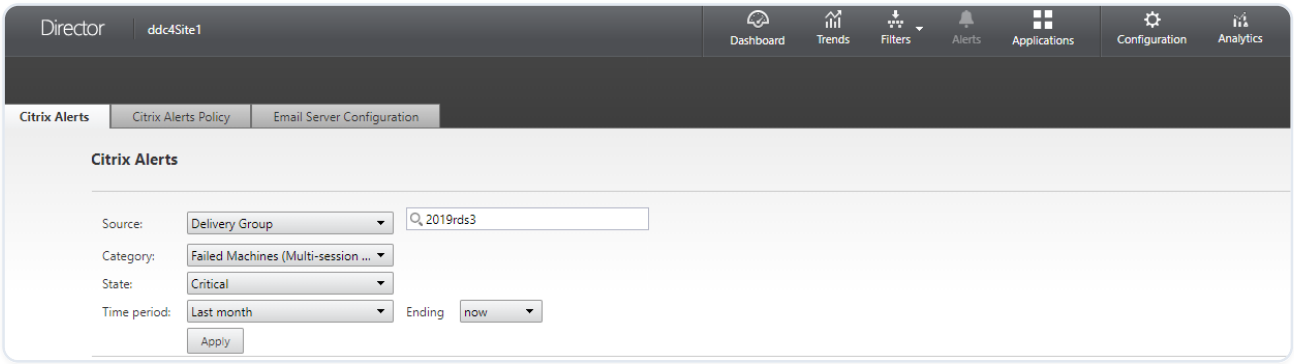


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre os alertas selecionando um alerta na barra lateral, clicando no link **Ir para Alertas** na parte inferior da barra lateral ou selecionando **Alertas** na parte superior da página do Director.

Na visualização Alertas, você pode filtrar e exportar alertas. Por exemplo, máquinas de SO multi-sessão com falha para um Delivery Group específico no último mês, ou todos os alertas para um usuário específico. Para obter mais informações, consulte Exportar relatórios.



Alertas do Citrix®

Os alertas Citrix são alertas monitorados no Director que se originam de componentes Citrix. Você pode configurar alertas Citrix no Director em **Alertas** \> **Política de Alertas Citrix**. Como parte da configuração, você pode definir notificações a serem enviadas por e-mail para indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar Alertas Citrix, consulte Criar políticas de alerta.

> **Observação:**
>
> Certifique-se de que seu firewall, proxy ou Microsoft Exchange Server não bloqueie os alertas por e-mail.

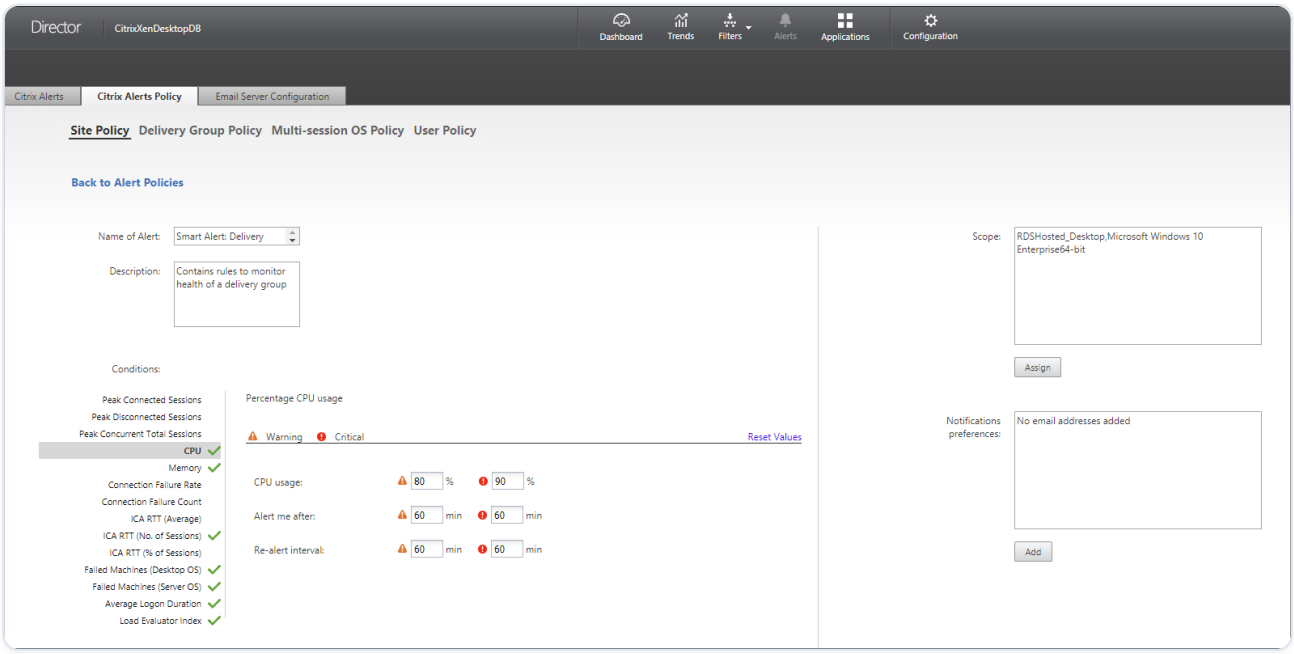
Políticas de alerta inteligentes

Um conjunto de políticas de alerta integradas com valores de limite predefinidos está disponível para Delivery Groups e escopo de VDA de SO multi-sessão. Esse 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 Delivery Group 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.

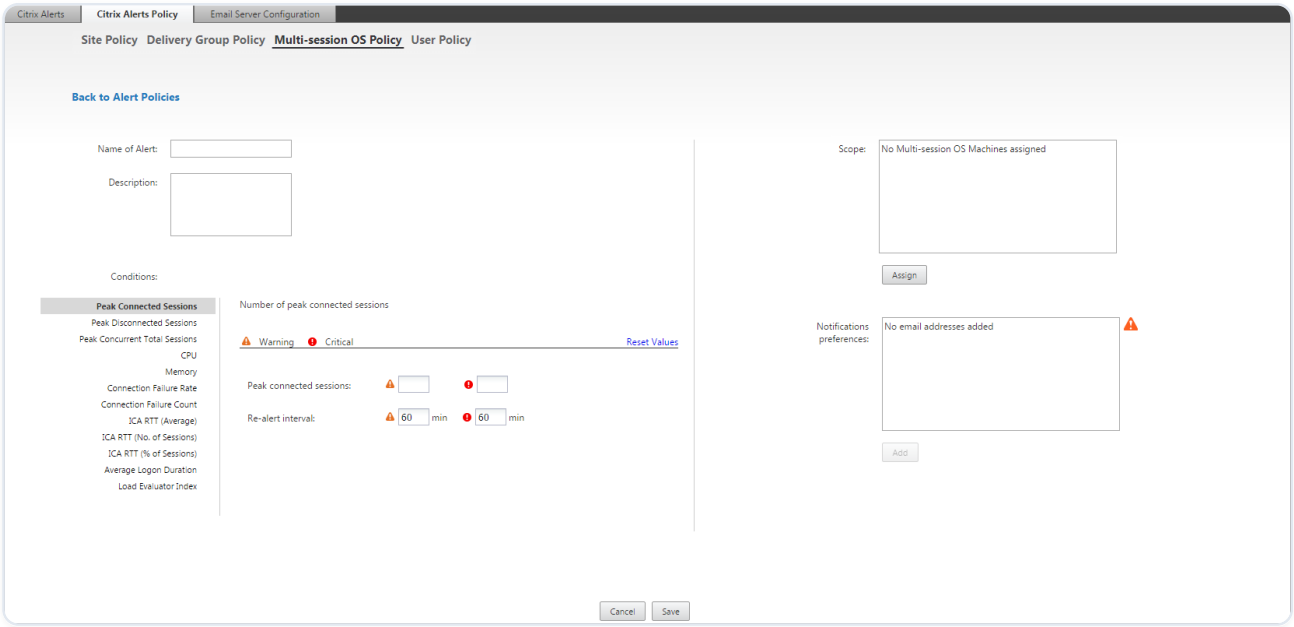


Alertas SCOM

Os alertas SCOM exibem informações de alerta do Microsoft System Center 2012 Operations Manager (SCOM) para fornecer uma indicação mais abrangente da saúde e desempenho do data center dentro do Director. Para obter mais informações, consulte a seção Configurar integração de alertas SCOM.

O número de alertas exibidos ao lado dos ícones de alerta antes de expandir a barra lateral é a soma combinada dos alertas Citrix e SCOM.

Criar políticas de alerta



Para criar uma nova política de alerta, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alertas** \> **Política de Alertas do Citrix** e selecione, por exemplo, Política de SO de Múltiplas Sessões.
2. Clique em **Criar**.
3. Nomeie e descreva a política, depois defina as condições que devem ser atendidas para que o alerta seja acionado. Por exemplo, especifique as contagens de Aviso e Crítico para Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico. Os valores de Aviso não devem ser maiores que os valores Críticos. Para obter mais informações, consulte Condições das políticas de alerta.
4. Defina o intervalo de Re-alerta. Se as condições para o alerta ainda forem atendidas, o alerta será acionado novamente neste intervalo de tempo e, se configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta ignorado não gera uma notificação por e-mail no intervalo de re-alerta.
5. Defina o Escopo. Por exemplo, defina para um Delivery Group específico.
6. Nas 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 spinner é exibido durante esse período.

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 (acima de 5 segundos).

Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro pode acionar alertas errôneos do Grupo de Entrega que são definidos usando parâmetros da máquina.

Condições das políticas de alertas

Encontre abaixo as categorias de alerta, as ações recomendadas para mitigar o alerta e as condições de política integradas, se definidas. As políticas de alerta integradas são definidas para intervalos de alerta e realerta de 60 minutos.

Pico de Sessões Conectadas

- Verifique a exibição Tendências de Sessão do Director para sessões conectadas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário

Pico de Sessões Desconectadas

- Verifique a exibição Tendências de Sessão do Director para sessões desconectadas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

Pico de Sessões Totais Concorrentes

- Verifique a exibição Tendências de Sessão 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 são acionados. Para obter mais informações, consulte Configurações da política de monitoramento
>
> **Condições de política inteligente:**
>
> - **Escopo:** Grupo de Entrega, escopo de SO multissessão
> - **Valores de limite:** Aviso - 80%, Crítico - 90%

Memória

A porcentagem de uso da memória indica o consumo geral de memória no VDA, incluindo o dos processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem memória. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Encerrar o processo causa a perda de dados não salvos.
- Se tudo estiver funcionando como esperado, adicione memória adicional no futuro.

> **Nota:**

> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se essa configuração de política estiver desabilitada, alertas com condições de CPU e memória não são acionados. Para obter mais informações, consulte Configurações da política de monitoramento

> **Condições de política inteligente:**

- **Escopo:** Grupo de Entrega, escopo de SO multissessão
- **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 obter um detalhamento 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 a Latência e determine se é um problema de rede ou um problema com aplicativos ou desktops.

ICA RTT (Nº de Sessões)

Número de sessões que excedem o tempo de ida e volta ICA limite.

- Verifique o Citrix ADM para o número de sessões com 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 multissessão
  - **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 vários motivos, conforme mostrado nas exibições Painel e Filtros do Director.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para mais informações, consulte Solucionar problemas do usuário.

  Condições de política inteligente:

  - **Escopo:** Escopo do Grupo de Entrega
  - **Valores de limite:** Aviso - 1, Crítico - 2

Máquinas com falha (SO multiusuário)

Número de máquinas de SO multissessão com falha. As falhas podem ocorrer por vários motivos, 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 multissessão
- **Valores de limite:** Aviso - 1, Crítico - 2

Duração Média do Logon

Duração média do logon para logons que ocorreram na última hora.

- Verifique o Painel do Director para obter métricas atualizadas sobre a duração do logon. Um grande número de usuários fazendo logon em um curto período pode aumentar a duração do logon.
- Verifique a linha de base e a análise 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 de 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 de 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 Citrix Hypervisor™ e VMware vSphere ajudam a monitorar os parâmetros e estados do hipervisor. O status da conexão com o hipervisor também é monitorado para fornecer um alerta se o cluster ou pool de hosts for reiniciado ou estiver indisponível.

Para receber alertas do hipervisor, certifique-se de que uma conexão de hospedagem seja criada no Citrix Studio. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas para alertas do hipervisor. A tabela a seguir descreve os vários parâmetros e estados dos alertas do hipervisor.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Uso da CPU	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da CPU é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de memória	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de memória é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de rede	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de rede é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de disco	VMware vSphere	Hypervisor	O limite de alerta de uso de disco é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Conexão do host ou estado de energia	VMware vSphere	Hypervisor	O Host do Hypervisor foi reiniciado ou está indisponível	Os alertas são pré-construídos no VMware vSphere. Nenhuma configuração adicional é necessária.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Conexão do Hypervisor indisponível	Citrix Hypervisor, VMware vSphere	Delivery Controller™	A conexão com o hypervisor (pool ou cluster) foi perdida, desligada ou reiniciada. Este alerta é gerado a cada hora enquanto a conexão estiver indisponível.	Os alertas são pré-construídos com o Delivery Controller. Nenhuma configuração adicional é necessária.

Nota:

Para obter mais informações sobre a configuração de alertas, consulte Alertas do Citrix XenCenter ou verifique a documentação de Alertas do VMware vCenter.

A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > site Policy > Hypervisor Health**. As condições de limite para as políticas de alerta do hipervisor 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.

Importante:

- Os alertas acionados pelo hipervisor são buscados e exibidos no Director. No entanto, as alterações no ciclo de vida/estado dos alertas do hipervisor não são refletidas no Director.
- Alertas que estão saudáveis, descartados ou desabilitados no console do Hypervisor continuam a aparecer no Director e devem ser descartados explicitamente.

- Alertas que são descartados no Director não são descartados automaticamente no console do Hypervisor.

Filtro de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/hypervisor_alerts_filter.png)

Uma nova categoria de Alerta chamada **Integridade do Hipervisor** foi adicionada para permitir a filtragem apenas dos alertas do hipervisor. Esses alertas são exibidos assim que os limites são atingidos ou excedidos. Os alertas do hipervisor podem ser:

- Crítico — limite crítico da política de alarme do hipervisor atingido ou excedido
- Aviso — limite de aviso da política de alarme do hipervisor atingido ou excedido
- Ignorado — alerta não mais exibido como um alerta ativo

Exibição de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2203-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.

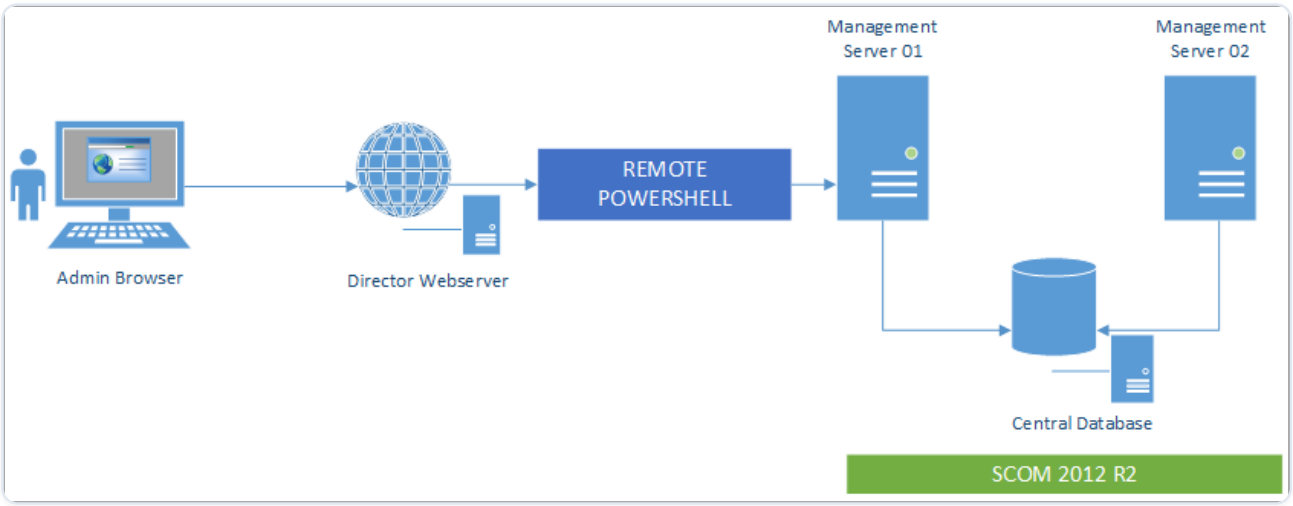
Configurar a integração de alertas SCOM

A integração do SCOM com o Director permite visualizar informações de alerta do SCOM no Dashboard e em outras visualizações de alto nível no Director.

Os alertas do SCOM são exibidos na tela junto com os alertas do Citrix. Você pode acessar e detalhar os alertas do SCOM na guia SCOM na barra lateral.

Você pode visualizar alertas históricos de até um mês, classificar, filtrar e exportar as informações filtradas para os formatos de relatório CSV, Excel e PDF. Para obter mais informações, consulte Exportar relatórios.

A integração do SCOM usa o PowerShell 3.0 remoto ou posterior para consultar dados do SCOM Management Server e mantém uma conexão de runspace persistente na sessão do Director do usuário. O Director e o servidor SCOM devem ter a mesma versão do PowerShell.



Os requisitos para a integração do SCOM são:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 ou posterior (a versão do PowerShell no Director e no servidor SCOM deve ser a mesma)
- CPU Quad Core com 16 GB de RAM (recomendado)
- Um Management Server primário para SCOM deve ser configurado no arquivo web.config do Director. Você pode fazer isso usando a ferramenta DirectorConfig.

A Citrix recomenda que a conta de administrador do Director seja configurada como uma função de Operador SCOM para que todas as informações de alerta possam ser recuperadas no Director. Se isso não for possível, uma conta de administrador SCOM pode ser configurada no arquivo web.config usando a ferramenta DirectorConfig.

A Citrix recomenda ainda que você não configure mais de 10 administradores do Director por SCOM Management Server para garantir o desempenho ideal.

No servidor Director:

1. Digite **Enable-PSRemoting** para habilitar o PowerShell remoting.
2. Adicione o SCOM Management Server à lista TrustedHosts. Abra um prompt do PowerShell e execute o(s) seguinte(s) comando(s):

    - Obtenha a lista atual de TrustedHosts

      Get-Item WSMAN:\localhost\Client\TrustedHosts

    - Adicione o FQDN do Servidor de Gerenciamento SCOM à lista de TrustedHosts. \<Old Values\> representa o conjunto existente de entradas retornadas do cmdlet Get-Item.

Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "\<FQDN SCOM Management Server\>,\<Old Values\>"

3. Configure o SCOM usando a ferramenta DirectorConfig.

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

No servidor de gerenciamento SCOM:

1. Atribua administradores do Director a uma função de administrador SCOM.

   a. Abra o console de gerenciamento SCOM e vá para **Administração** \> **Segurança** \> **Funções de Usuário**.

   b. Em Funções de Usuário, você pode criar uma nova Função de Usuário ou modificar uma existente. Existem quatro categorias de funções de operador SCOM que definem a natureza do acesso aos dados do SCOM. Por exemplo, uma função Somente Leitura não vê o painel de Administração e não pode descobrir ou gerenciar regras, máquinas ou contas. Uma função de Operador é uma função de administrador completo.

      > **Observação:**
      >
      > As seguintes operações não estão disponíveis se o administrador do Director for atribuído a uma função que não seja de operador:
      >
      > - Se houver vários servidores de gerenciamento configurados e o servidor de gerenciamento primário não estiver disponível, o administrador do Director não poderá se conectar ao servidor de gerenciamento secundário. O servidor de gerenciamento primário é o servidor configurado no arquivo web.config do Director, ou seja, o mesmo servidor especificado com a ferramenta DirectorConfig na etapa 3 acima. Os servidores de gerenciamento secundários são servidores de gerenciamento pares do servidor primário.
      > - Ao filtrar alertas, o administrador do Director não pode pesquisar a origem do alerta. Isso requer uma permissão de nível de operador.

   c. Para modificar qualquer Função de Usuário, clique com o botão direito do mouse na função e, em seguida, clique em **Propriedades**.

   d. Na caixa de diálogo Propriedades da Função de Usuário, você pode adicionar ou remover administradores do Director da função de usuário especificada.

2. Adicione administradores do Director ao grupo Usuários de Gerenciamento Remoto no servidor de gerenciamento SCOM. Isso permite que os administradores do Director estabeleçam uma conexão remota do PowerShell.
3. Digite **Enable-PSRemoting** para habilitar o acesso remoto do PowerShell.
4. Defina os limites de propriedades do WS-Management:

   a. Modifique MaxConcurrentUsers:

      Na CLI:

      ```
      winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
      ```

      No PS:

      ```
      Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
      ```

   b. Modifique MaxShellsPerUser:

      Na CLI:

      ```
      winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
      ```

      No PS:

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
   ```

   a. Modifique MaxMemoryPerShellMB:

      Na CLI:

      ```
      winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
      ```

      Em PS:

   ```
   Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
   ```

5. Para garantir que a integração do SCOM funcione em ambientes de domínio misto, defina a seguinte entrada de registro.

Caminho:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

Chave: LocalAccountTokenFilterPolicy

Tipo: DWord

Valor: 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.

Uma vez que a integração do SCOM esteja configurada, você poderá ver a mensagem "Não é possível obter os alertas SCOM mais recentes. Consulte os logs de eventos do servidor Director para obter mais informações". Os logs de eventos do servidor ajudam a identificar e corrigir o problema. As causas podem incluir:

- Perda de conectividade de rede na máquina do Director ou do SCOM.
- O serviço SCOM não está disponível ou está muito ocupado para responder.
- Autorização falha devido a uma alteração nas permissões para o usuário configurado.
- Um erro no Director durante o processamento dos dados do SCOM.
- Incompatibilidade de versão do PowerShell entre o Director e o servidor SCOM.

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.

- **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 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 para enviar mensagens.
10. Nas exibições **Máquinas** e **Conexões**, clique em **Motivo da Falha** de uma máquina ou conexão com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de Máquina e Conexão estão disponíveis no Guia de Solução de Problemas de Motivos de Falha do Citrix Director 7.12.
11. Na exibição de **Máquinas**, clique em um link de nome de máquina para ir para a página correspondente de **Detalhes da Máquina**. Esta página exibe os detalhes da máquina, fornece controles de energia, exibe os gráficos de monitoramento de CPU, memória, disco e GPU. Além disso, clique em **Exibir Utilização Histórica** para ver as tendências de utilização de recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
12. Na exibição **Instâncias de Aplicativo**, classifique ou filtre com base no **Tempo Ocioso** maior que um período 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 Citrix 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 com licença não Premium e não 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 de tempo é definido como Último mês (**Terminando agora**) ou menor. Para o período de tempo escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendências estão disponíveis como gráficos e não como tabelas.
- Os valores de retenção de limpeza do Monitor Service 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

Ver tendências para sessões: Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas de Confiabilidade da Sessão ou 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 perfeita. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período selecionado nos Filtros. Um detalhamento fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Este recurso requer o Delivery Controller™ versão 7 1906 ou posterior, e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações 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 Controladores de Entrega descartam as cargas úteis 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 visualização 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 de 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 que é 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 somente 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 visualização 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 visualização 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.

> **Nota:**
>
> Muitos processos listados nesta tabela podem consumir uma grande quantidade de dados, afetando o desempenho. Para evitar isso, são listados apenas os processos com CPU Média ou Memória Média superior a 1%. Assim, a tabela pode, às vezes, listar menos de 10 processos.

> Filtre por Grupo de Entrega e Período. Os gráficos de CPU, uso de 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 Top 10 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).

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 visualização contextual de usuário, aplicativo e desktop da rede. 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

Visualizar falhas de aplicativo: A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. São suportados VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de múltiplas sessões executando Windows Server 2008 e posterior. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas as falhas de aplicativo de VDAs de SO de múltiplas sessões são exibidas. Você pode definir o monitoramento de falhas de aplicativo usando políticas de monitoramento. Para obter mais informações, consulte Configurações da política de monitoramento.

Visualizar resultados da sondagem de aplicativos: A guia Resultados da Sondagem de Aplicativos exibe os resultados da sondagem para aplicativos que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha de inicialização do aplicativo ocorreu é registrado.

Este recurso requer Delivery Controller(s) e VDAs **versão 7.18** ou posterior. Para obter mais informações, consulte Sondagem de aplicativos.

Criar relatórios personalizados: A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados em tempo real e históricos do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatórios Personalizados salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente, ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique as 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 na Visualização e no relatório de 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:**

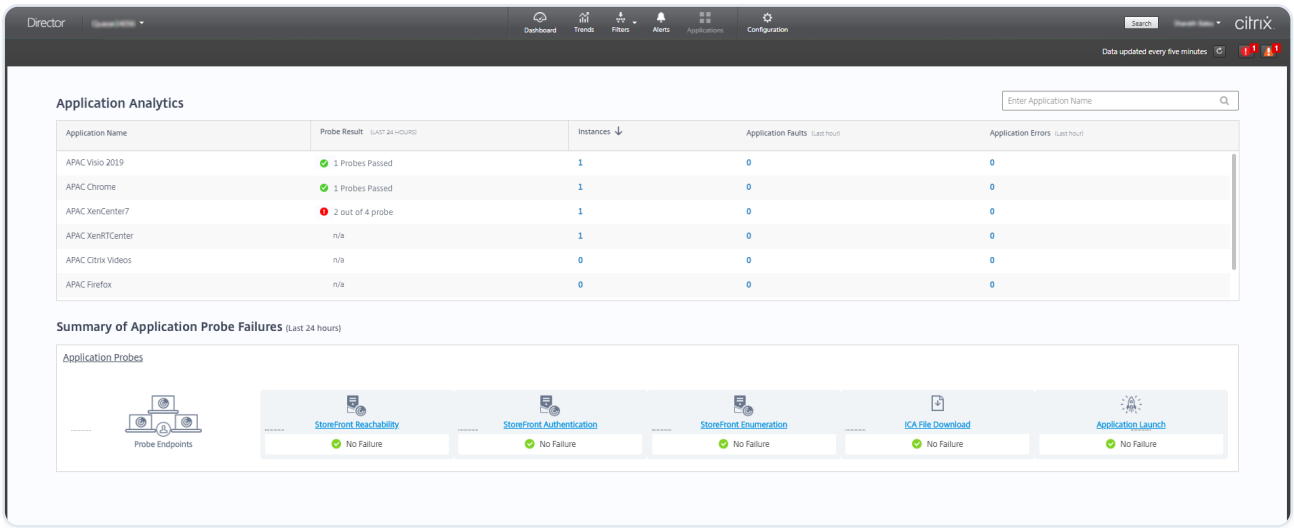
- Os dados de logon da conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
- Os Grupos de Entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros de Tendências do Director até que os dados relacionados a 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.

Solucionar problemas de implantações

Solucionar problemas de aplicativos

Análise de Aplicativos

A exibição **Aplicativos** mostra análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho de aplicativos 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.

A coluna **Instâncias** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativos atualmente em execução (instâncias conectadas e desconectadas). Para solucionar problemas adicionais, clique no campo **Instâncias** para ver a página de filtros correspondente **Instâncias de Aplicativos**. Aqui, você pode selecionar instâncias de aplicativos para fazer logoff ou desconectar.

> **Nota:**
>
> Para administradores de escopo personalizado, o Director não exibe instâncias de aplicativos criadas em grupos de aplicativos. Para visualizar todas as instâncias de aplicativos, você deve ser um administrador completo. Para obter mais informações, consulte o artigo do Knowledge Center CTX256001.

> Monitore a integridade dos aplicativos publicados em seu site com as colunas **Falhas de Aplicativos** e **Erros de Aplicativos**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao iniciar o aplicativo correspondente na última hora. Clique no campo **Falhas de Aplicativos** ou **Erros de Aplicativos** para ver os detalhes da falha na página **Tendências** \> **Falhas de Aplicativos** correspondente ao aplicativo selecionado.

As configurações da política de falha de aplicativo governam a disponibilidade e a exibição de falhas e erros. Para obter mais informações sobre as políticas e como modificá-las, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da **política de monitoramento**.

Monitoramento de aplicativos em tempo real

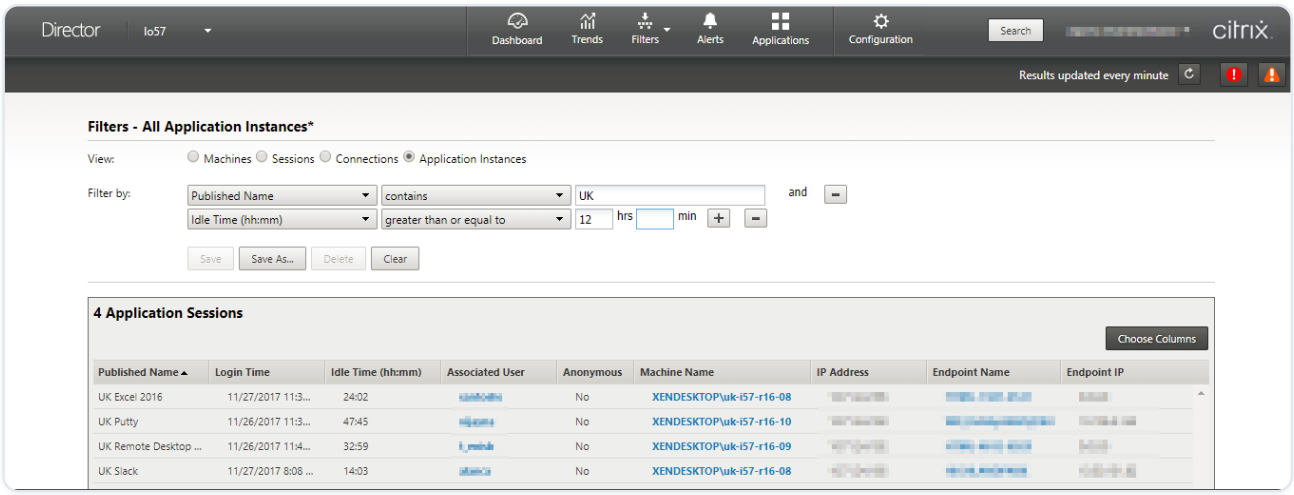
Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas baseada em aplicativos são no setor de saúde, onde os funcionários compartilham licenças de aplicativos. Lá, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente Citrix Virtual Apps and Desktops™, reconfigurar servidores com baixo desempenho ou manter e atualizar aplicativos.

A página de filtro **Instâncias de Aplicativos** lista todas as instâncias de aplicativos em VDAs de SO de Servidor e de Sessão Única. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativos em VDAs de SO de Múltiplas Sessões que estiveram ociosas por pelo menos 10 minutos.

Nota: As métricas de Instâncias de Aplicativos estão disponíveis em sites de todas as edições de licença.

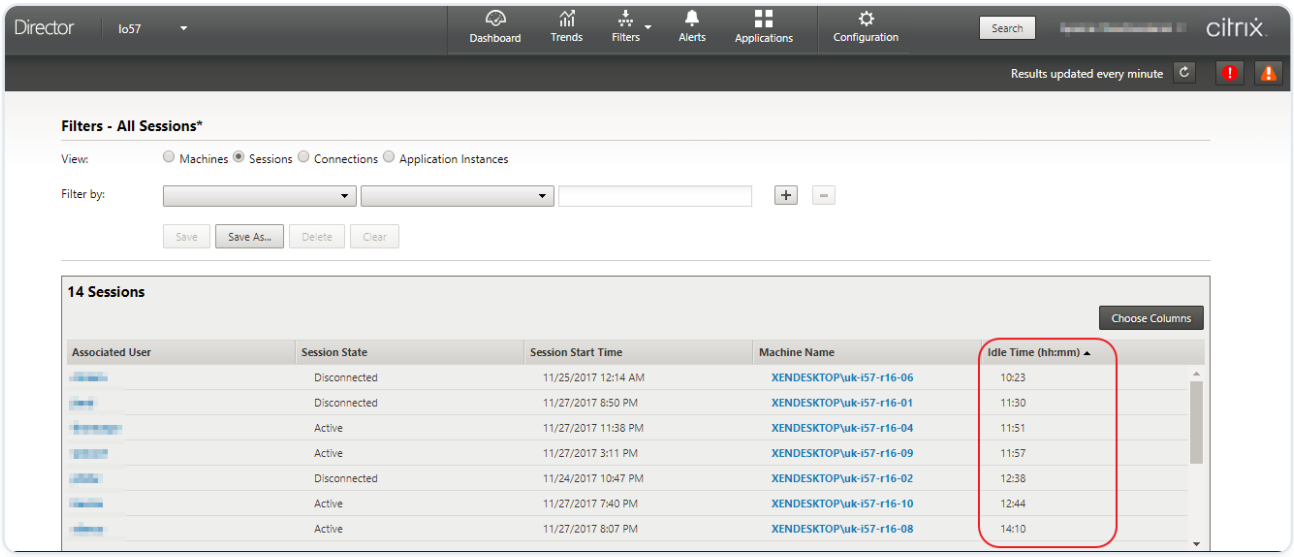
Use essas informações para identificar as instâncias de aplicativos que estão ociosas além de um período de tempo específico e faça logoff ou desconecte-as conforme apropriado. Para fazer isso, selecione **Filtros \> Instâncias de Aplicativos** e selecione um filtro pré-salvo ou escolha **Todas as Instâncias de Aplicativos** e crie seu próprio filtro.



Um exemplo de filtro seria o seguinte. Como critérios de **Filtrar por**, escolha **Nome Publicado** (do aplicativo) e **Tempo Ocioso**. Em seguida, defina **Tempo Ocioso** como **maior ou igual a** um limite de tempo específico e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias do aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Controle de Sessão**, escolha **Logoff** ou **Desconectar** para encerrar as instâncias.

Nota: Fazer logoff ou desconectar uma instância de aplicativo faz logoff ou desconecta a sessão atual, encerrando assim todas as instâncias de aplicativo que pertencem à mesma sessão.

Você pode identificar sessões ociosas na página de filtro **Sessões** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Tempo Ocioso** ou defina um filtro para identificar sessões que estão ociosas além de um limite de tempo específico. O tempo ocioso é listado para sessões em VDAs de SO de múltiplas sessões que estiveram ociosas por pelo menos 10 minutos.



O **Tempo ocioso** é exibido como **N/A** quando a sessão ou instância do aplicativo

- não está ociosa há 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.

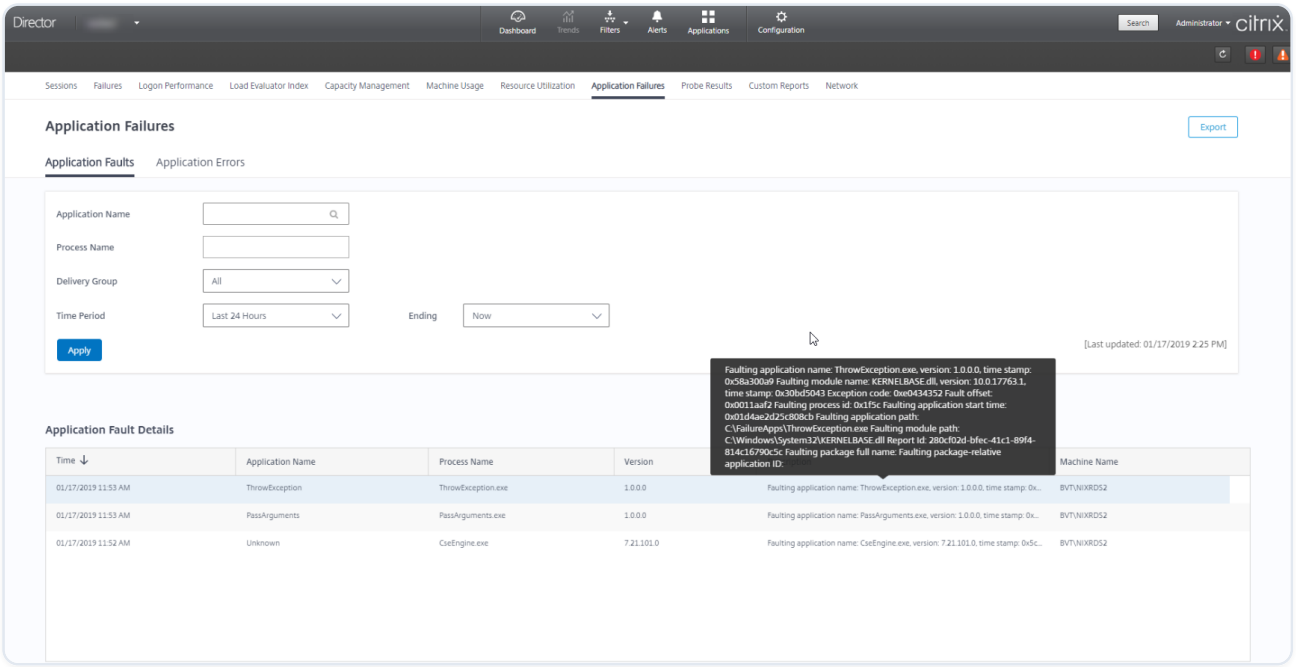
Monitoramento histórico de falhas de aplicativo

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 "Erros de Aplicativo" são monitoradas. Clique em **Exportar** para gerar relatórios nos formatos CSV, Excel ou PDF

As configurações de retenção de limpeza para monitoramento de falhas de aplicativos, GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays, são definidas como um dia por padrão para sites com licença Premium e não Premium. Você pode alterar essa configuração usando o comando PowerShell:

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```



As falhas são exibidas como **Falhas de Aplicativo** ou **Erros de Aplicativo** com base em sua gravidade. A guia Falhas de Aplicativo exibe falhas associadas à perda de funcionalidade ou dados. Erros de Aplicativo indicam problemas que não são imediatamente relevantes; eles significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Nome do Aplicativo Publicado**, **Nome do Processo** ou **Grupo de Entrega** e **Período de Tempo**. A tabela exibe o código da falha ou erro e uma breve descrição da falha. A descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:** O nome do aplicativo publicado é exibido como “Desconhecido” quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de desktop ou quando falha devido a uma exceção não tratada causada por um executável dependente.

> Por padrão, apenas falhas de aplicativos hospedados em VDAs de SO de 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 nas configurações da política de monitoramento.

A página **Tendências \> Resultados da Sondagem de Aplicativos** exibe os resultados da sondagem de aplicativos executada no site nas últimas 24 horas e 7 dias. Para obter mais detalhes sobre como configurar sondagens de aplicativos, consulte Sondagem de Aplicativos.

Sondagem de aplicativos

A sondagem de aplicativos automatiza o processo de verificação da integridade dos Citrix Virtual Apps™ que são publicados em um site. Os resultados da sondagem de aplicativos estão disponíveis no Director.

Requisitos:

- O Delivery Controller executa a versão 7.18 ou posterior.
- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com Citrix Receiver para Windows Versão 4.8 ou posterior, ou Citrix Workspace app para Windows (anteriormente Citrix Receiver para Windows) Versão 1808 ou posterior. O Workspace app para Unified Windows Platform (UWP) não é compatível.
- O Director e o StoreFront™ suportam a autenticação baseada em formulário padrão.

Contas de usuário/permissões necessárias para executar a Sondagem de Aplicativos:

- Um usuário exclusivo do StoreFront para sondar em cada máquina de endpoint. O usuário do StoreFront não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint
- Uma conta de usuário de administrador completo ou uma função personalizada com as seguintes permissões. A reutilização de contas de usuário existentes para sondagem de aplicativos pode desconectar os usuários de suas sessões ativas.
    - Permissões de grupo de entrega:
        - Somente leitura
    - Permissões 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

Configurar Sondagem de Aplicativos

Você pode agendar suas sondagens de aplicativos para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados aos aplicativos, à máquina de hospedagem ou à conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 suporta agregação de sites. Aplicativos e desktops podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o agente de sondagem, selecione a opção **Agregação de Sites do Workspace (StoreFront) Ativada** para habilitar a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

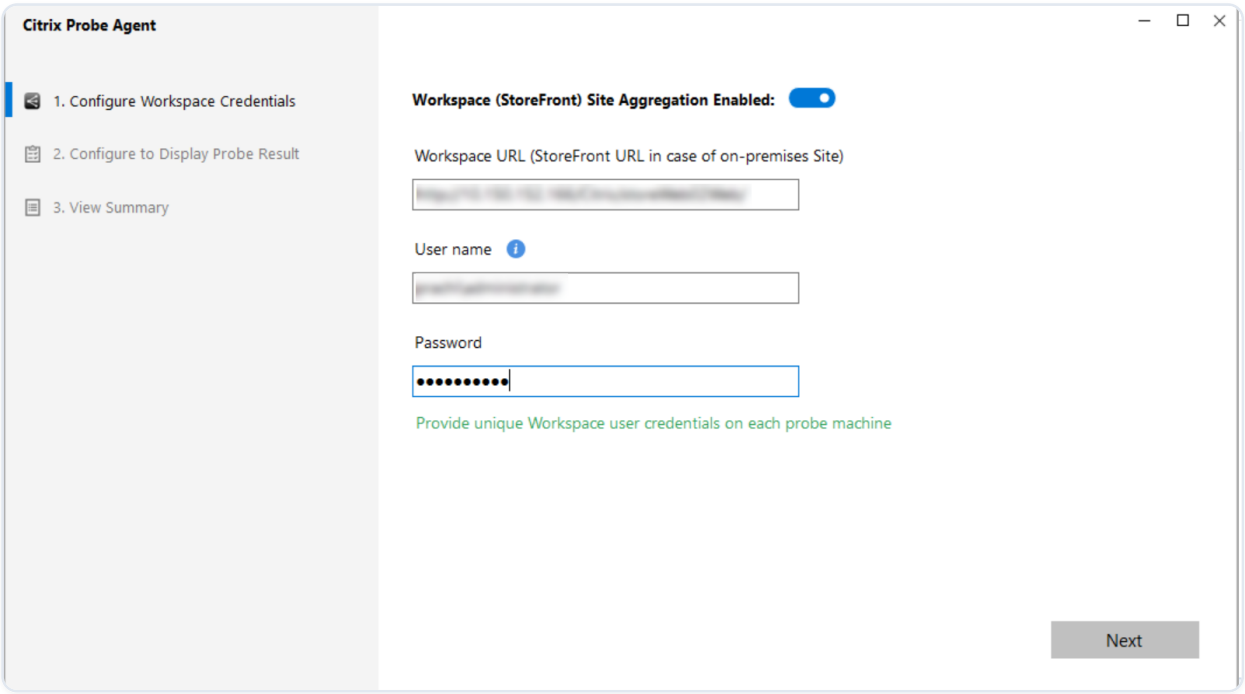
- Vários sites locais com uma URL do StoreFront.
- Sites locais e na nuvem com uma URL do StoreFront ou do Workspace.
- Vários sites na nuvem com uma URL do Workspace.

> **Observação:**
>
> Você deve criar administradores ou usuários separados para configurar sondas que tenham acesso a apenas um site.

ETAPA 1: INSTALAR E CONFIGURAR O CITRIX PROBE AGENT

O Citrix Probe Agent é um executável do Windows que simula o lançamento real de aplicativos pelo usuário através do StoreFront. Ele testa os lançamentos de aplicativos conforme configurado no Director e reporta os resultados de volta ao Director.

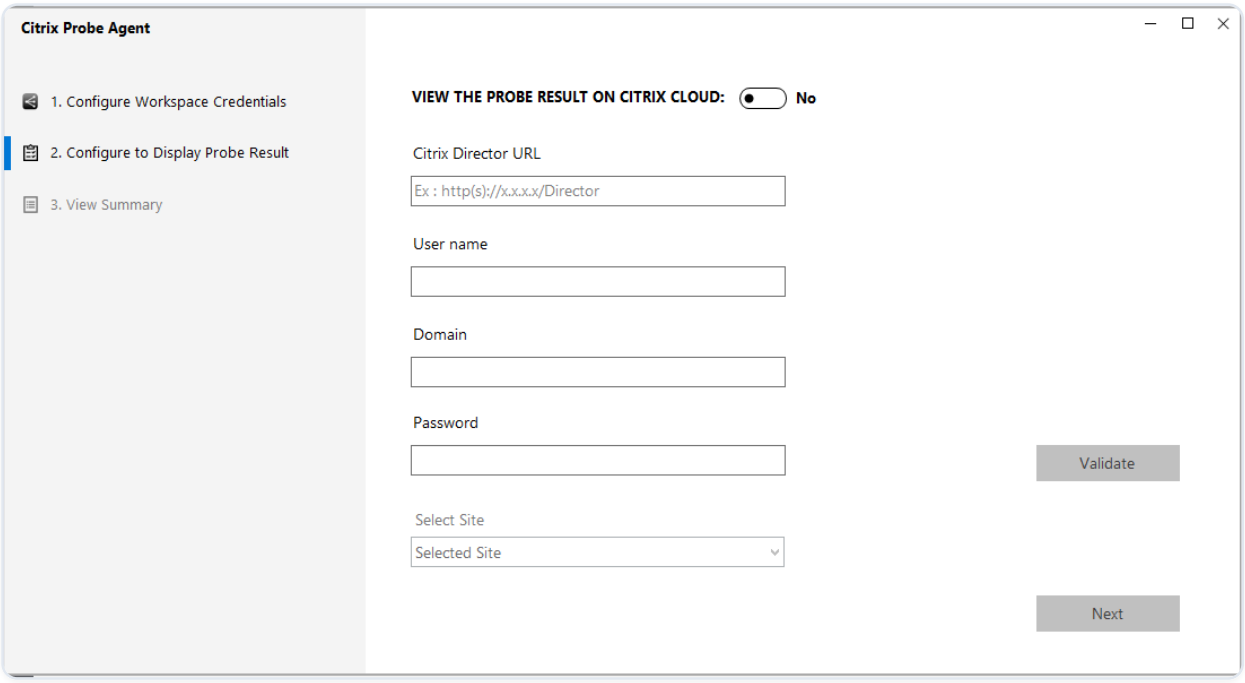
1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem de aplicativos.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`
3. Inicie o agente e configure suas credenciais do StoreFront Receiver para Web. Configure um usuário StoreFront exclusivo em cada máquina de endpoint. As credenciais são criptografadas e armazenadas com segurança.



Observação:

Para acessar o site a ser sondado de fora da rede, digite a URL de login do Citrix Gateway no campo URL do StoreFront. O Citrix Gateway roteia automaticamente a solicitação para a URL do StoreFront do site correspondente. Este recurso está disponível para o Citrix Gateway versão 12.1 e posterior (tema RfWebUI) e Delivery Controllers 1811 e posterior.

4. Na guia **Configurar para Exibir Resultado da Sondagem**, insira suas credenciais do Director e clique em **Validar**.



5. Selecione seu site e clique em **Avançar**.

ETAPA 2: CONFIGURAR SONDAGEM DE APLICATIVOS NO DIRECTOR

Limitação:

A sondagem falha se os aplicativos 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 desabilitar a mensagem de logon em um VDA de Servidor. Vá para Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança.

Remova o texto nos seguintes campos e atualize a política da Microsoft.

- Logon Interativo: Texto da Mensagem para usuários tentando fazer logon
- Logon Interativo: Título da Mensagem para usuários tentando fazer logon

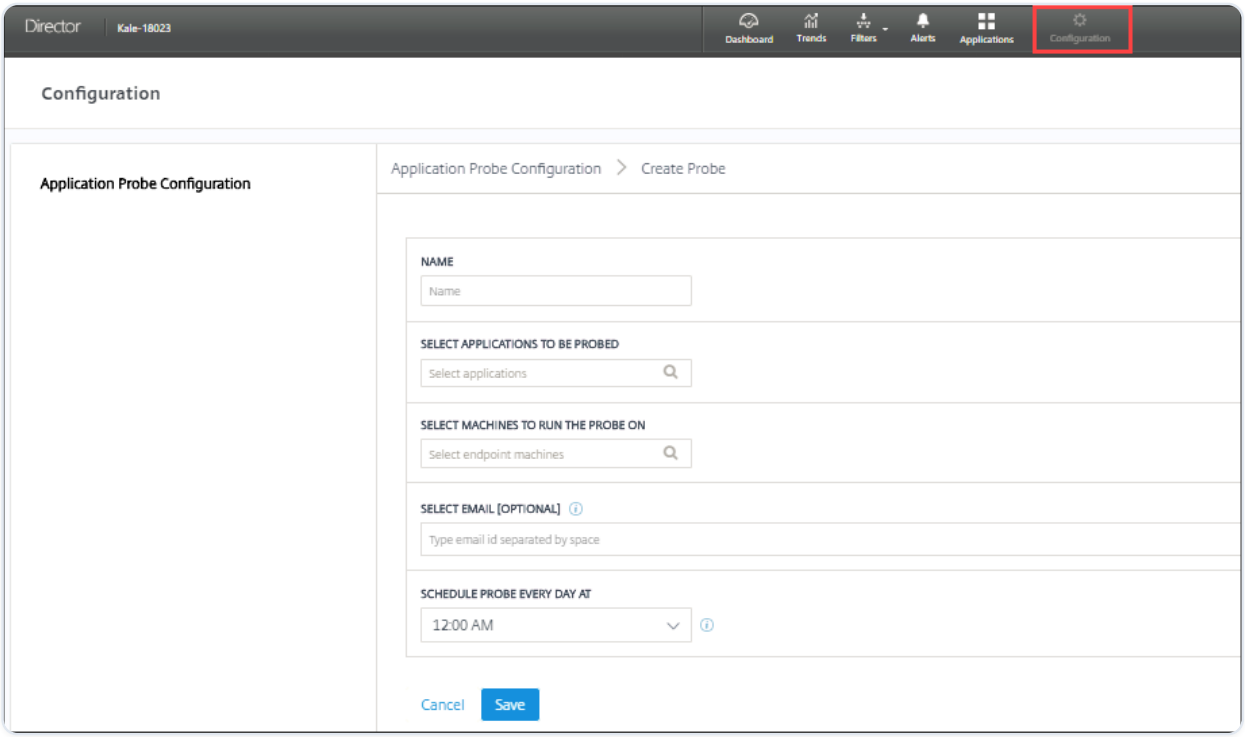
Atribua o usuário da sondagem a este VDA de Servidor específico com o banner de mensagem de logon interativo desabilitado para garantir que a sondagem possa passar do estado de Inicialização do Aplicativo.

> Para obter mais informações, consulte `<https://learn.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`.

1. Vá para **Configuração** \> **Configuração da Sondagem de Aplicativos**.
2. Crie uma sonda e escolha:

   - os aplicativos a serem sondados,
   - as máquinas de endpoint nas quais a sondagem deve ser executada,
   - os endereços de e-mail para os quais os resultados da sondagem de falha são enviados (configure seu servidor de e-mail em **Alertas** -\> **Configuração do Servidor de E-mail**), e
   - a hora do dia em que a sondagem deve ser executada (de acordo com o fuso horário local da máquina de endpoint).

   Após a configuração no Director, o agente leva 10 minutos antes de estar pronto para iniciar a sondagem. Em seguida, ele executa as sondas configuradas a partir da próxima hora.



ETAPA 3: EXECUÇÃO DA SONDA

O agente executa a sondagem de aplicativos de acordo com a configuração de sondagem que ele busca periodicamente do Director. Ele inicia os aplicativos selecionados serialmente usando o StoreFront. O agente reporta os resultados de volta ao Director através do banco de dados Monitor. As falhas são reportadas em cinco estágios específicos:

- **Acessibilidade do StoreFront** - a URL do StoreFront configurada não está acessível.
- **Autenticação do StoreFront** - as credenciais do StoreFront configuradas são inválidas.
- **Enumeração do StoreFront** - a lista de aplicativos de enumeração do StoreFront não contém o aplicativo a ser sondado.
- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização do aplicativo** – o aplicativo não pode ser iniciado.

ETAPA 4: VISUALIZAR RESULTADOS DA SONDA

Você pode visualizar os resultados mais recentes da sondagem na página **Aplicativos**.

Página de Análise de Aplicativos do Director(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-app-analytics.png)

Para solucionar problemas adicionais, clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** \> **Resultados da Sondagem de Aplicativos**.

Resultados da sondagem de aplicativos do Director(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-app-probing-trends.png)

Os dados consolidados dos resultados da sondagem estão disponíveis para os períodos das últimas 24 horas ou dos últimos 7 dias nesta página. Você pode ver o estágio em que a sondagem falhou. Você pode filtrar a tabela por um aplicativo específico, estágio de falha da sondagem ou máquina de endpoint.

Sondagem de desktops

A sondagem de desktops automatiza o processo de verificação da integridade dos Citrix Virtual Desktops™ publicados em um site. Os resultados da sondagem de desktops estão disponíveis no Director.

Na página de Configuração do Director, configure os desktops a serem sondados, as máquinas de endpoint para executar a sondagem e o tempo da sondagem. O agente testa o lançamento dos desktops selecionados usando o StoreFront™ e reporta os resultados de volta ao Director. Os resultados da sondagem são exibidos na interface do usuário do Director – os dados das últimas 24 horas na página Applications e os dados históricos da sondagem na página **Trends > Probe Results > Desktop Probe Results**. Aqui, você pode ver o estágio em que a falha da sondagem ocorreu - StoreFront Reachability, StoreFront Authentication, StoreFront Enumeration, ICA download ou Desktop launch. O relatório de falha é enviado para os endereços de e-mail configurados. Você pode agendar suas sondagens de desktop para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes podem ajudar a

solucionar proativamente problemas relacionados a desktops provisionados, máquinas de hospedagem ou conexões antes que os usuários os experimentem. A sondagem de desktops está disponível para sites com licença Premium. Este recurso requer Delivery Controllers versão 7 1906 ou posterior e Probe Agent 1903 ou posterior.

Requisitos:

- O Delivery Controller™ executa a versão 1906 ou posterior.
- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com Citrix Receiver para Windows Versão 4.8 ou posterior, ou Citrix Workspace app para Windows (anteriormente Citrix Receiver para Windows) Versão 1906 ou posterior. O Workspace app para Unified Windows Platform (UWP) não é suportado.
- O Director e o StoreFront suportam a autenticação baseada em formulário padrão.

Contas de usuário ou permissões necessárias para executar a sondagem de desktops:

- Um usuário StoreFront exclusivo para sondar em cada máquina de endpoint. O usuário StoreFront não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint
- Uma conta de usuário administrador completa ou uma função personalizada com as seguintes permissões. A reutilização de contas de usuário normais para sondagem de desktops pode desconectar os usuários de suas sessões ativas.
    - 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

Configurar a sondagem de desktops

Você pode agendar suas sondagens de desktop para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados a desktops, máquinas de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 suporta agregação de sites. Aplicativos e desktops podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o agente de sondagem, selecione a opção **Agregação de Sites do Workspace (StoreFront) Ativada** para habilitar a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

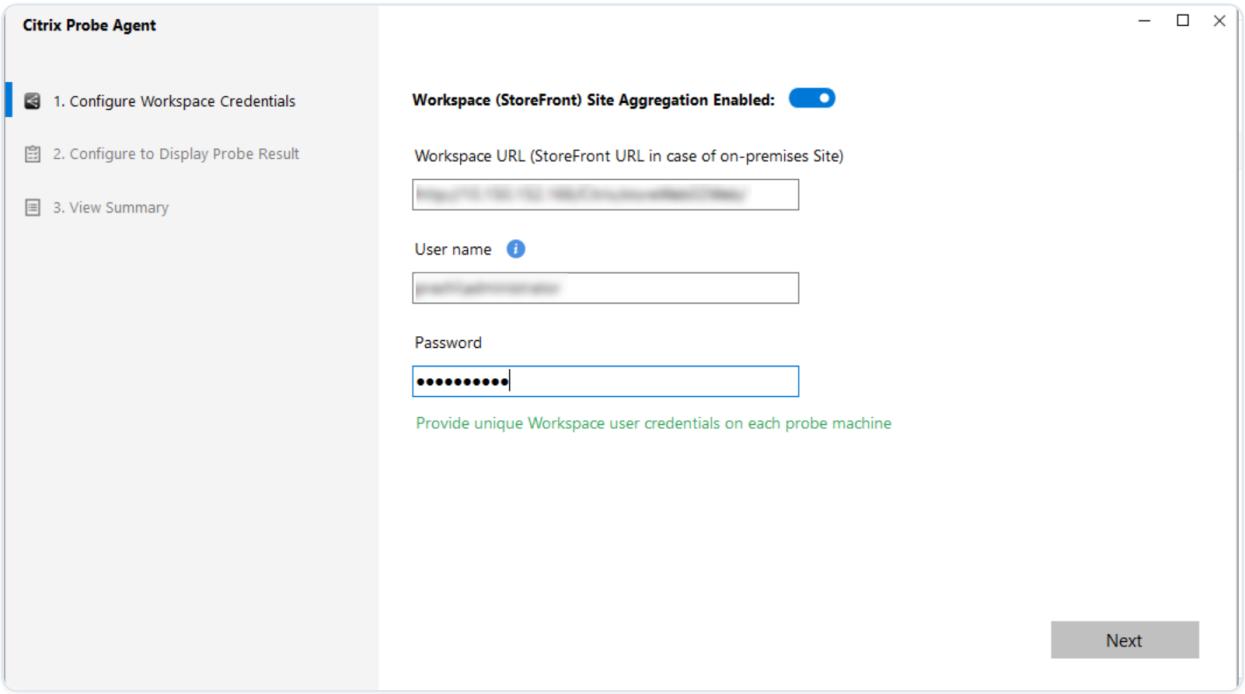
- Vários sites locais com uma URL do StoreFront.
- Locais no local e na nuvem que possuem um URL de StoreFront ou Workspace.
- Vários sites na nuvem com um URL de Workspace.

> **Observação:**
>
> 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 da área de trabalho pelo usuário através do StoreFront. Ele testa os lançamentos da área de trabalho conforme configurado no Director e reporta os resultados de volta ao Director.

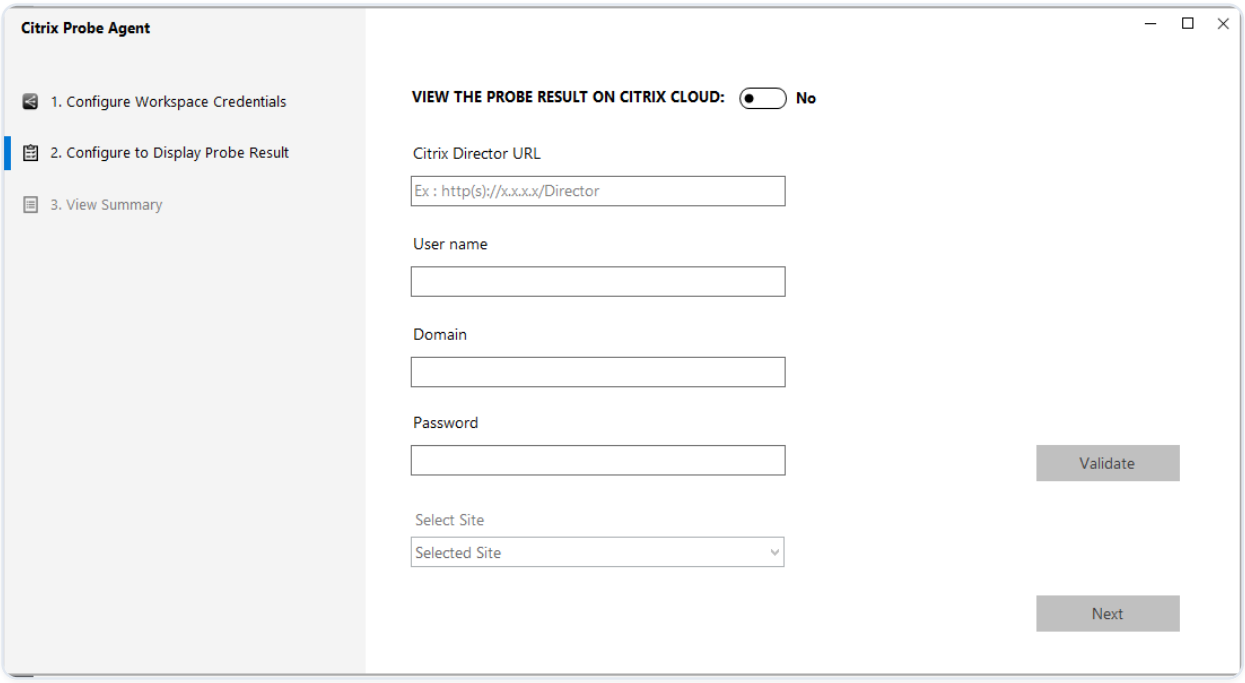
1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem de área de trabalho.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`
3. Inicie o agente e configure suas credenciais do StoreFront Receiver para Web. Configure um usuário StoreFront exclusivo em cada máquina de endpoint. As credenciais são criptografadas e armazenadas com segurança.



Observação:

- Para acessar o site a ser sondado de fora da rede, digite o URL da página de login do Citrix Gateway no campo URL do StoreFront. O Citrix Gateway roteia automaticamente a solicitação para o URL do StoreFront do site correspondente. Este recurso está disponível para o Citrix Gateway versão 12.1 ou posterior e Delivery Controllers 1811 ou posterior.
- Você deve habilitar o Logon Interativo para o usuário StoreFront exclusivo configurado.

4. Na guia **Configurar para Exibir Resultado da Sondagem**, insira suas credenciais do Director e clique em **Validar**.



5. Selecione seu site e clique em **Avançar**.

ETAPA 2: CONFIGURAR A SONDAGEM DE ÁREA DE TRABALHO NO DIRECTOR

Limitação:

A sondagem falha se as áreas de trabalho forem lançadas para teste a partir de VDAs do Windows que têm o banner de mensagem de logon interativo habilitado. Isso ocorre porque um tempo limite acontece devido à espera para aceitar a mensagem de logon interativo. Para desabilitar a mensagem de logon em um VDA de Servidor. Vá para Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de segurança.

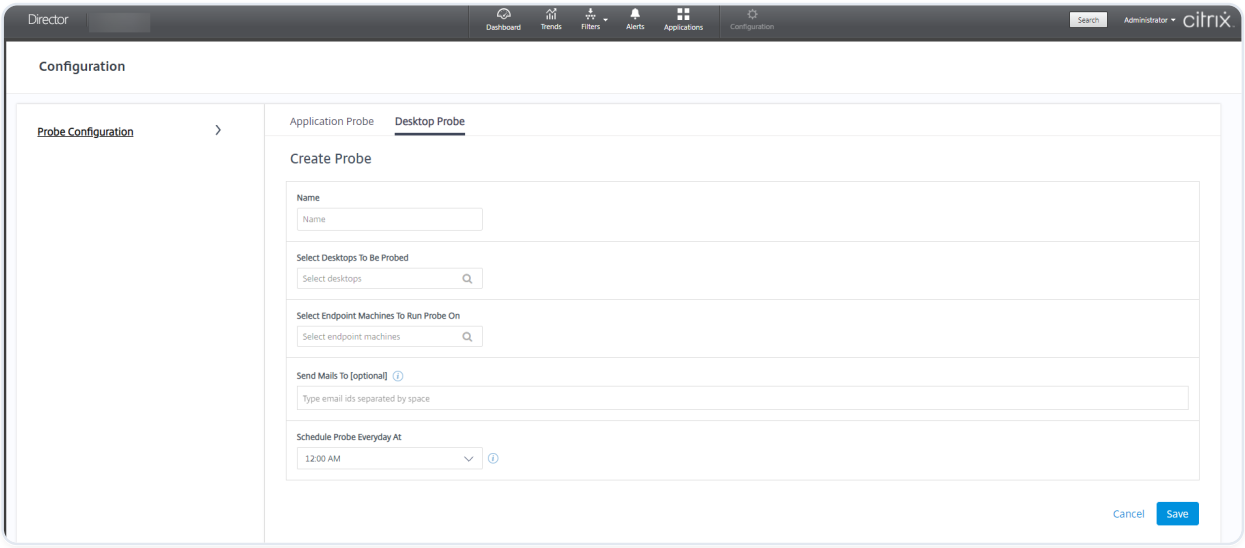
Remova o texto nos seguintes campos e atualize a política da Microsoft.

- Logon Interativo: Texto da Mensagem para usuários tentando fazer logon
- Logon Interativo: Título da Mensagem para usuários tentando fazer logon

Atribua o usuário da sondagem a este VDA de Servidor específico com o banner de mensagem de logon interativo desabilitado para garantir que a sondagem possa passar do estado de Lançamento da 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 **Configuração** > **Configuração da Sondagem de Área de Trabalho**.
2. Para criar uma sondagem, insira os detalhes e clique em **Salvar**.



Observação:

Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.

Após a conclusão da configuração da sondagem de desktop, o agente leva 10 minutos antes de estar pronto para iniciar a sondagem. Em seguida, ele executa as sondagens configuradas a partir da próxima hora.

ETAPA 3: EXECUÇÃO DA SONDAGEM

O agente executa a sondagem de desktop de acordo com a configuração de sondagem que ele busca periodicamente do Director. Ele inicia os desktops selecionados serialmente usando o StoreFront. O agente reporta os resultados de volta ao Director por meio do banco de dados 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 desktops enumerados do StoreFront não contém o desktop a ser sondado.

- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização do desktop** – o desktop não pode ser iniciado.

ETAPA 4: VISUALIZAR RESULTADOS DA SONDA

Você pode visualizar os resultados mais recentes da sondagem na página **Desktops**.

Página de Análise de Desktop do Director(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-desktop-probe-results.png)

Para solucionar problemas adicionais, clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** > **Resultados da Sondagem** > **Resultados da Sondagem de Desktop**.

Resultados da sondagem de desktop do Director(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-desktop-probing-trends.png)

Os dados consolidados dos resultados da sondagem estão disponíveis para os períodos das últimas 24 horas ou dos últimos 7 dias nesta página. Você pode ver o estágio em que a sondagem falhou. Você pode filtrar a tabela por um desktop específico, estágio de falha da sondagem ou máquina de endpoint.

Solucionar problemas de máquinas

> **Nota:**
>
> **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 da Central de Conhecimento, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém o download da ferramenta **Citrix Health Assistant** e instruções de uso.

> A exibição **Filtros > Máquinas** no console do Director exibe as máquinas configuradas no site. A guia Máquinas de SO de Múltiplas Sessões inclui o índice do avaliador de carga, que indica a distribuição dos contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.

Clique na coluna **Motivo da Falha** de uma máquina com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de máquina e conexão estão disponíveis no Guia de Solução de Problemas de Motivos de Falha do Citrix Director 7.12.

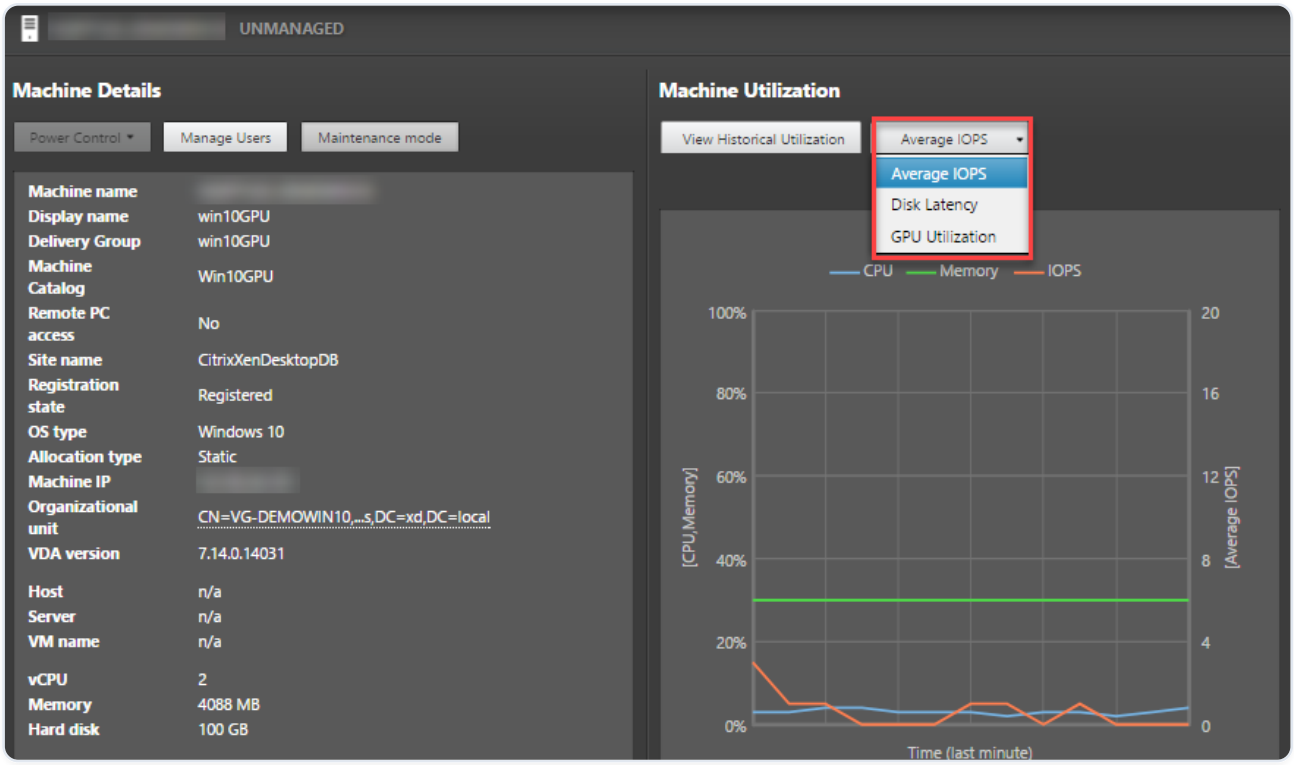
Clique no link do nome da máquina para ir para a página **Detalhes da Máquina**.

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 você 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.



Selecione **Utilização da GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do Codificador e Decodificador para solucionar problemas relacionados à GPU em VDAs de SO de Servidor ou de Sessão Única. Os gráficos de Utilização da GPU estão disponíveis apenas para

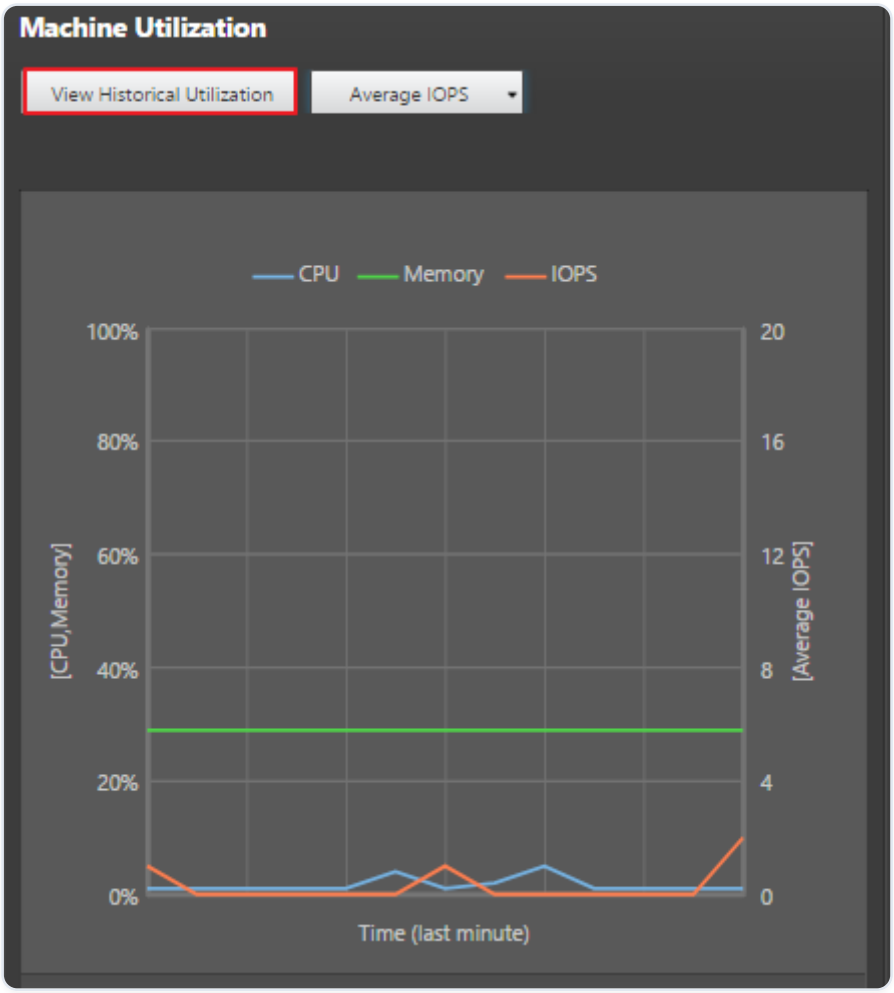
VDAs que executam Windows de 64 bits com GPUs NVIDIA Tesla M60 e que executam a versão 369.17 ou posterior do Driver de Vídeo. Os VDAs devem ter o HDX™ 3D Pro habilitado para fornecer aceleração de GPU. Para obter mais informações, consulte Aceleração de GPU para SO de Sessão Única do Windows e Aceleração de GPU para SO de Múltiplas Sessões do Windows. 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.

Utilização histórica de recursos baseada em máquina

No painel **Utilização da Máquina**, clique em **Exibir Utilização Histórica** para ver o uso histórico de recursos na máquina selecionada. Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, sessões simultâneas de pico, IOPS médio e latência de disco.

> **Nota:**
>
> A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como Permitido para coletar e exibir dados na tabela dos 10 Principais Processos na página de Utilização Histórica da Máquina. A coleta é proibida por padrão.

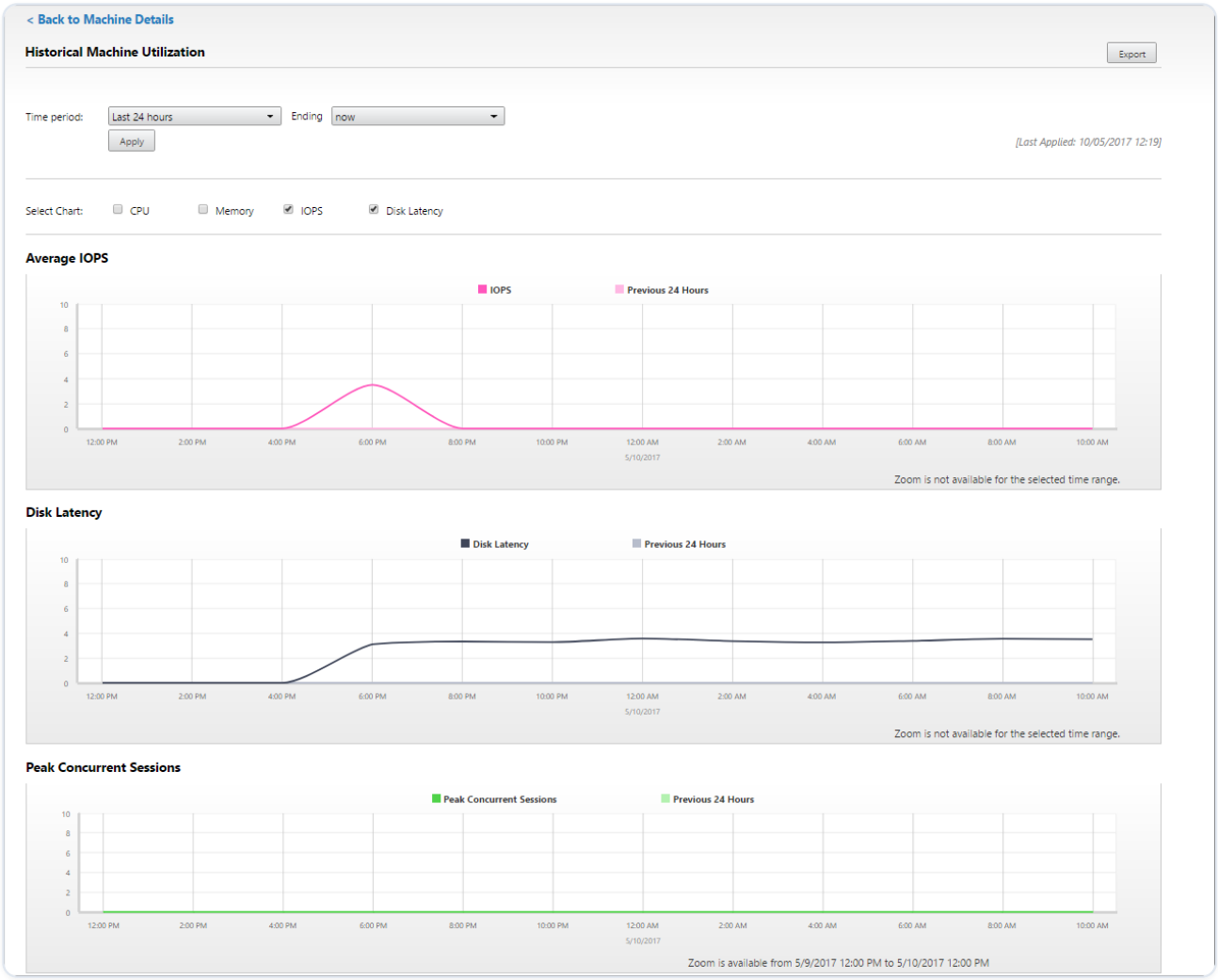
> Os dados de utilização de CPU e memória, IOPS médio e latência de disco são coletados por padrão. Você pode desabilitar a coleta usando a configuração da política **Habilitar Monitoramento de Recursos**.



1. No painel **Utilização da Máquina** na exibição **Detalhes da Máquina**, selecione **Exibir Utilização Histórica**.
2. Na página **Utilização Histórica da Máquina**, defina o **Período de Tempo** para visualizar o uso das últimas 2 horas, 24 horas, 7 dias, mês ou ano.

> **Nota:**
>
> Os dados de uso de IOPS médios 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 são as 2 horas anteriores ao intervalo de tempo selecionado. Visualize a tendência de CPU, memória e sessão nas últimas 2 horas e no tempo de linha de base. Se você selecionar **Último mês**, o período de linha de base é o mês anterior. Selecione para visualizar os IOPS médios e a latência de disco no último mês e no tempo de linha de base.

1. Clique em **Exportar** para exportar os dados de utilização de recursos para o período selecionado. Para obter mais informações, consulte a seção Exportar relatórios em Monitorar Implantações.
2. Abaixo dos gráficos, a tabela lista os 10 principais processos com base na utilização da CPU ou da memória. Você pode classificar por qualquer uma das colunas, que mostram Nome do Aplicativo, Nome de Usuário, ID da Sessão, CPU Média, Pico de CPU, Memória Média e Pico de Memória no intervalo de tempo selecionado. As colunas IOPS e Latência de Disco não podem ser classificadas.

> **Nota:**

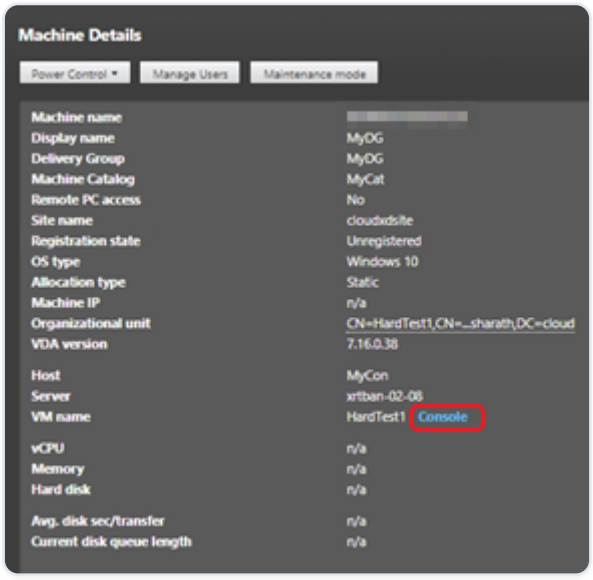
> O ID da sessão para processos do sistema é exibido como "0000".

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 multissessão 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 esse recurso esteja disponível:

- É necessário o Delivery Controller Versão 7.16 ou posterior.
- O XenServer que hospeda a máquina deve ser da Versão 7.3 ou posterior e deve estar acessível a partir da interface do usuário do Director.



Para solucionar problemas de uma máquina, clique no link **Console** no painel Detalhes da Máquina correspondente. Após a autenticação das credenciais do host que você fornecer, o console da máquina será 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 com SO de várias 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 Microsoft RDS excedeu seu período de carência.
Erro	Um Servidor de Licenças não está configurado para o nível de SO exigido com o tipo de licenciamento de Acesso de Cliente Por Dispositivo.
Erro	O Servidor de Licenças configurado é incompatível com o nível de SO do Host RDS com o tipo de licenciamento de Acesso de Cliente Por Dispositivo.
Aviso	O Servidor de Terminal Pessoal não é um tipo de licenciamento RDS válido em uma implantação do Citrix Virtual Apps and Desktops™.
Aviso	O Remote Desktop 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.

TIPO DE MENSAGEM	MENSAGENS NO DIRECTOR
Aviso	O Controlador de Domínio ou Servidor de Licenças está inacessível com o tipo de licenciamento RDS de Acesso de Cliente Por Usuário.
Aviso	Com o tipo de licenciamento de Acesso de Cliente Por Dispositivo, a licença do Dispositivo Cliente não pode ser determinada, já que o servidor de licenças para o nível de SO exigido está inacessível.

Nota:

Este recurso é aplicável apenas para Microsoft RDS CAL (Licença de Acesso para Cliente).

Solucionar problemas do usuário

Use a exibição **Help Desk** (página **Activity Manager**) do Director para visualizar informações sobre o usuário:

- Verifique os detalhes sobre o logon, a conexão e os aplicativos do usuário.
- Acompanhe a máquina do usuário.
- Grave a sessão ICA®.
- Solucione o problema com as ações recomendadas na tabela a seguir e, se necessário, escale o problema para o administrador apropriado.

Dicas de solução de problemas

PROBLEMA DO USUÁRIO	SUGESTÕES
O logon demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de logon do usuário
A inicialização da sessão demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de inicialização da sessão
O aplicativo está lento ou não responde	Resolver falhas de aplicativo

PROBLEMA DO USUÁRIO	SUGESTÕES
A conexão falhou	Restaurar conexões de desktop
A sessão está lenta ou não está respondendo	Restaurar sessões
Gravar sessões	Gravar sessões
O vídeo está lento ou com baixa qualidade	Executar relatórios do sistema de canal HDX

> **Nota:** Para garantir que a máquina não esteja no modo de manutenção, na exibição Detalhes do Usuário, revise o painel Detalhes da Máquina.

Dicas de pesquisa

Quando você digita o nome do usuário em um campo de Pesquisa, o Director pesquisa usuários no Active Directory para usuários em todos os sites configurados para oferecer suporte ao Director.

Quando você digita um nome de máquina multiusuário em um campo de Pesquisa, o Director exibe os Detalhes da Máquina para a máquina especificada.

Quando você digita um nome de endpoint em um campo de Pesquisa, o Director usa as sessões não autenticadas (anônimas) e autenticadas que estão conectadas a um endpoint específico, o que 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.

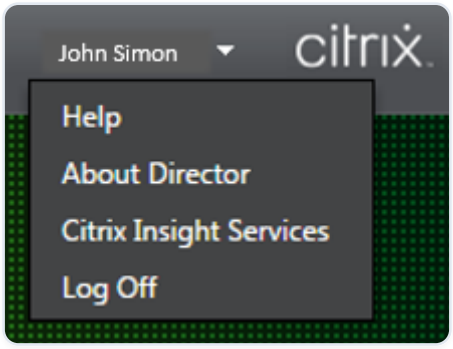
Os resultados da pesquisa também incluem usuários que não estão usando ou atribuídos a uma máquina no momento.

- As pesquisas não diferenciam maiúsculas de minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome composto (nome de usuário, sobrenome e primeiro nome ou nome de exibição), separados por um espaço, os resultados incluem correspondências para ambas as strings. 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 extras. 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 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 Inicial, selecione Citrix \> Citrix Scout.

Para obter informações sobre como usar e configurar o Scout, e para perguntas frequentes, consulte CTX130147.

Diagnosticar problemas de inicialização de sessão

Além das fases do processo de logon mencionadas na seção Diagnosticar problemas de logon do usuário, o Director exibe a duração da inicialização da sessão. Isso é dividido em duração de Inicialização da Sessão do Workspace App e Inicialização da Sessão 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. Esse recurso está disponível no Delivery Controller versão 7 1906 e posterior e em 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.

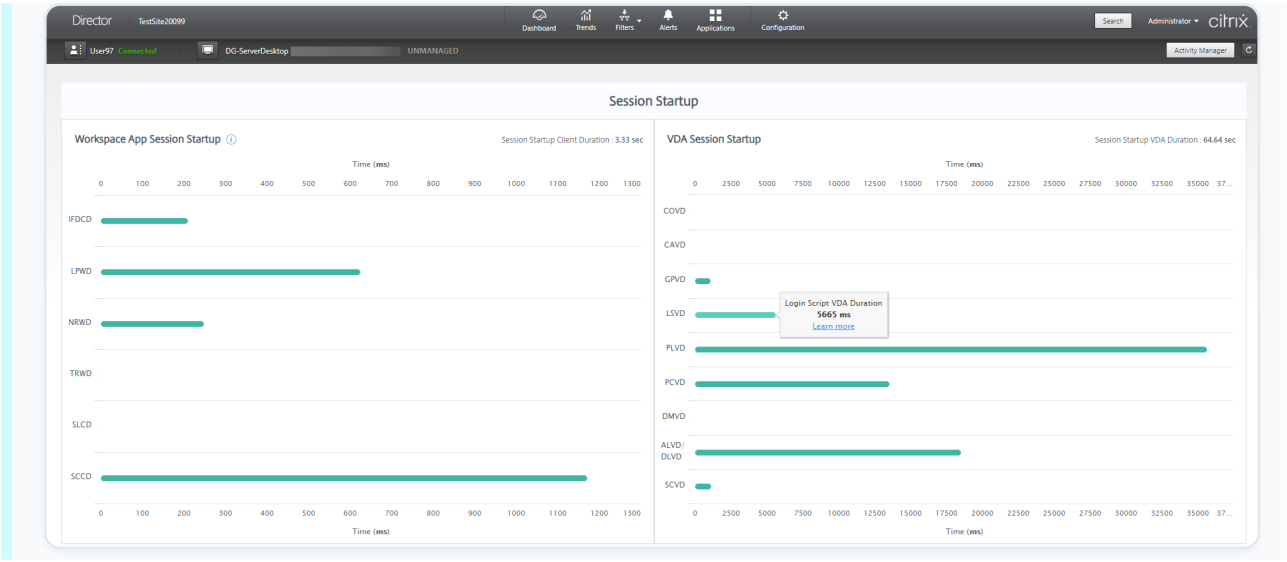
Limitações

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 do Download do Arquivo ICA® (IFDCD) está disponível apenas quando o Workspace App é detectado ao iniciar a partir de um navegador.
- Para inicializações de sessão de macOS, o IFDCD está disponível apenas para o Workspace App 1902 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 para a inicialização do aplicativo mais recente.
- Algumas métricas na Inicialização da Sessão VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.



Fases de inicialização da sessão do Workspace App

DURAÇÃO DA INICIALIZAÇÃO DA SESSÃO DO CLIENTE (SSCD)

Quando essa métrica é alta, indica um problema do lado do cliente que está causando tempos de inicialização longos. Revise as métricas subsequentes para determinar a provável causa raiz do problema. O SSCD começa o mais próximo possível do momento da solicitação (clique do mouse). 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, já que grande parte dos custos de configuração associados à criação de uma nova conexão com o servidor não são incorridos. No nível seguinte, há várias métricas detalhadas disponíveis.

DURAÇÃO DO DOWNLOAD DO ARQUIVO ICA (IFDCD)

Este é o tempo levado para o cliente baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou desktop) no aplicativo Workspace.
2. Uma solicitação do usuário é enviada ao StoreFront™ através do Citrix Gateway (se configurado), que envia a solicitação ao Delivery Controller.
3. O Delivery Controller encontra uma máquina disponível para a solicitação e envia as informações da máquina e outros detalhes para o StoreFront. Além disso, o StoreFront solicita e recebe um tíquete único da Secure Ticket Authority.
4. O StoreFront gera um arquivo ICA e o envia ao usuário via Citrix Gateway (se configurado).

O IFDCD representa o tempo que leva para o processo completo (etapas 1–4). 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 lado do servidor do lançamento 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. Então, você pode solucionar problemas de rede potenciais primeiro.

DURAÇÃO DO SERVIDOR WEB DA PÁGINA DE LANÇAMENTO (LPWD)

Este é o tempo levado para processar a página de lançamento (launch.aspx) no StoreFront. Se o LPWD for alto, pode haver um gargalo no StoreFront.

As possíveis causas incluem:

- 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 está alta, isso indica que o Delivery Controller está demorando muito para resolver o nome de um aplicativo publicado para um endereço IP.

As possíveis causas incluem um problema no cliente, problemas com o Delivery Controller, 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 DA PESQUISA DE SESSÃO DO CLIENTE (SLCD)

Esta duração representa o tempo gasto para consultar cada sessão para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode manipular a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

DURAÇÃO DA CRIAÇÃO DE SESSÃO DO CLIENTE (SCCD)

Esta duração representa o tempo gasto para criar uma sessão, desde o momento em que o wfica32.exe (ou um arquivo equivalente similar) é iniciado até o momento em que a conexão é estabelecida.

Fases de inicialização da sessão VDA

DURAÇÃO DE INICIALIZAÇÃO DA SESSÃO VDA (SSVD)

Esta duração é a métrica de inicialização de conexão de alto nível do lado do servidor que engloba o tempo que o VDA leva para executar 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 executando 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 necessário 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 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, especificamente quando os usuários têm muitas impressoras locais. Para fazer isso, edite a política de criação automática de impressoras no Delivery Controller e no Citrix Virtual Apps and Desktops.

DURAÇÃO DO MAPEAMENTO DE UNIDADE VDA (DMVD)

Este é o tempo levado pelo VDA para mapear as unidades cliente, dispositivos e portas do usuário.

Certifique-se de que suas políticas base incluam configurações para desabilitar canais virtuais não utilizados. Por exemplo, mapeamento de áudio ou porta COM, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

DURAÇÃO DO LANÇAMENTO DE APLICATIVO/DESKTOP VDA (ALVD/DLVD)

Esta fase é uma combinação da duração do Userinit e do Shell. Quando um usuário faz logon em uma máquina Windows, o winlogon executa userinit.exe. 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 o desktop virtual ou aplicativo.

A duração do Shell é o tempo entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

DURAÇÃO DA CRIAÇÃO DE SESSÃO VDA (SCVD)

Este tempo inclui qualquer atraso diverso no tempo de criação da sessão no VDA.

Diagnosticar problemas de logon do usuário

Use os dados de Duração de Logon para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a um desktop ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o Protocolo de Área de Trabalho Remota ou reconectar-se de sessões desconectadas. Especificamente, a duração do logon não é medida quando um usuário se conecta inicialmente usando um protocolo não-HDX e se reconecta usando HDX.

Na exibição Detalhes do Usuário, a duração é exibida como um valor numérico. Abaixo desse número, é exibido o horário em que o logon ocorreu e um gráfico das fases do processo de logon.

À medida que os usuários fazem logon no Citrix Virtual Apps and Desktops™, o Serviço de Monitoramento rastreia as fases do processo de logon. As fases começam a partir do momento em que o usuário se conecta do aplicativo Citrix Workspace™ até o momento em que a área de trabalho está pronta para uso.

O número grande à esquerda é o tempo total de logon. Isso é calculado combinando o tempo gasto para estabelecer a conexão e obter uma área de trabalho do Delivery Controller™ com o tempo gasto para autenticar e fazer logon em uma área de trabalho virtual. As informações de duração são apresentadas em segundos (ou frações de segundos).

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração do logon e os detalhamentos apareçam:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Serviço de Gerenciamento de Perfil do Citrix esteja em execução.
3. Para sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Não processar a lista de execução herdada**.
4. O rastreamento de processo de auditoria deve ser habilitado para o detalhamento da Sessão Interativa.

5. Para o detalhamento de GPO, aumente o tamanho dos logs operacionais da Política de Grupo.

Notas:

- A duração do logon é suportada apenas no shell padrão do Windows (explorer.exe) e não em shells personalizados.
- A duração do logon para Acesso Remoto ao PC está disponível somente 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 ao PC. Para obter mais informações, consulte a Etapa 4 em Considerações sobre configuração e sequência do Acesso Remoto ao PC.

Etapas para solucionar problemas de logon do usuário

1. Na exibição **Detalhes do Usuário**, solucione o estado do logon usando o painel Duração do Logon.
    - Se o usuário estiver fazendo logon, a exibição reflete o processo de logon.
    - Se o usuário estiver logado, o painel Duração do Logon exibe o tempo que o usuário levou para fazer logon na sessão atual.
2. Examine as fases do processo de logon.

Fases do processo de logon

INTERMEDIAÇÃO

Tempo levado para decidir qual desktop atribuir ao usuário.

INICIALIZAÇÃO DA 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

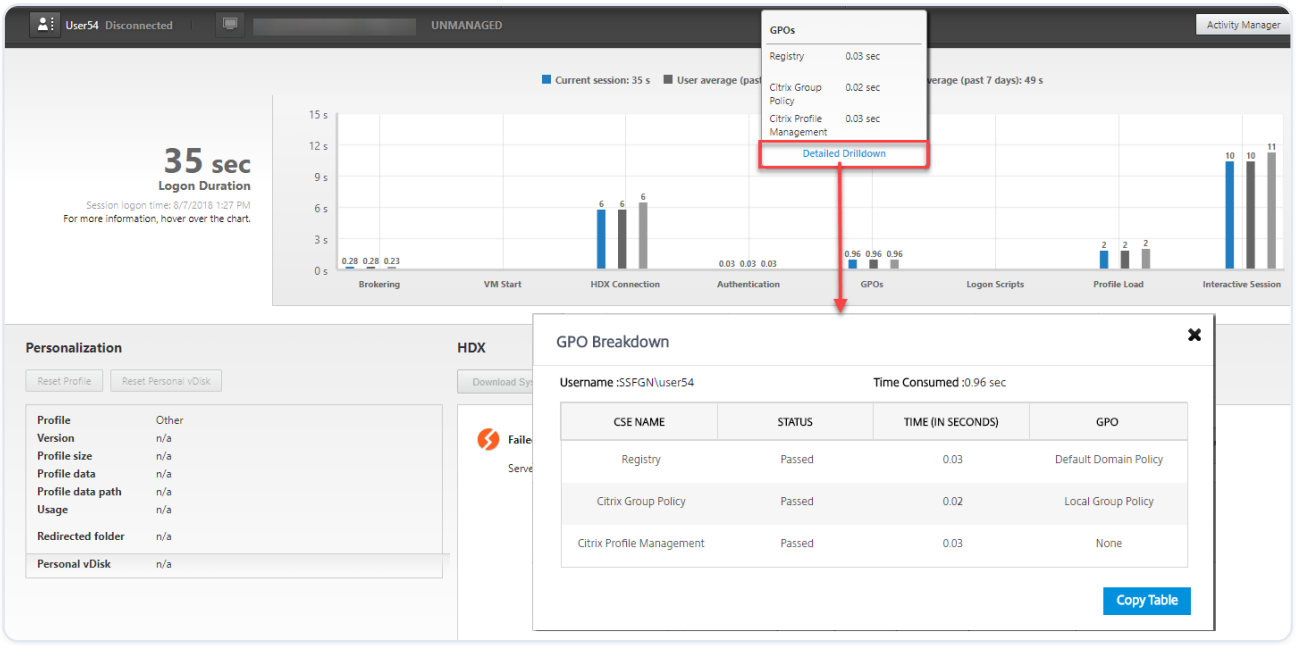
Tempo necessário para concluir as etapas exigidas na configuração da conexão HDX do cliente para a máquina virtual.

AUTENTICAÇÃO

Tempo necessário para concluir a autenticação na sessão remota.

GPOS

Se as configurações de Política de Grupo estiverem habilitadas nas máquinas virtuais, este é o tempo necessário para aplicar os objetos de política de grupo durante o logon. O detalhamento do tempo necessário para aplicar cada política de acordo com as CSEs (Extensão do Lado do Cliente) está disponível como uma dica de ferramenta ao passar o mouse sobre a barra GPO.



Clique em **Detalhamento Detalhado** 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 da CSE e não se somam ao 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 Configurando os Logs de Eventos.

SCRIPTS DE LOGON

Se os scripts de logon estiverem configurados para a sessão, este é o tempo necessário para que os scripts de logon sejam executados.

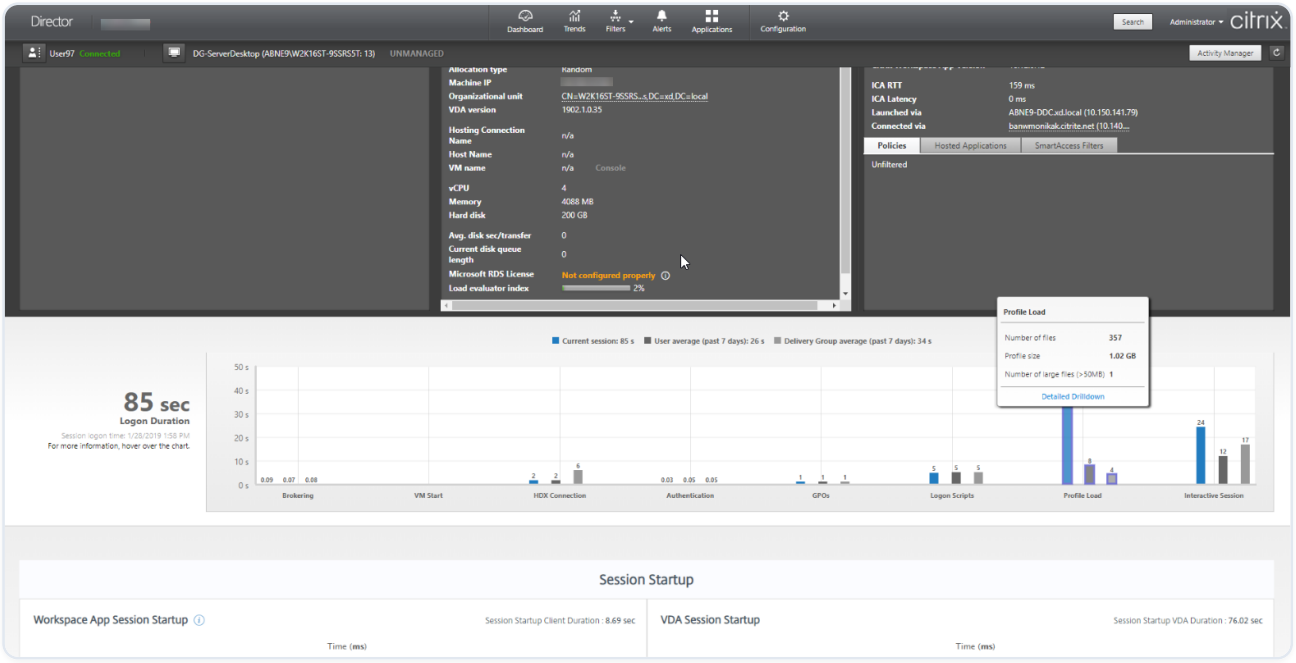
CARREGAMENTO DE PERFIL

Se as configurações de perfil estiverem configuradas para o usuário ou a máquina virtual, este é o tempo necessário para o perfil carregar.

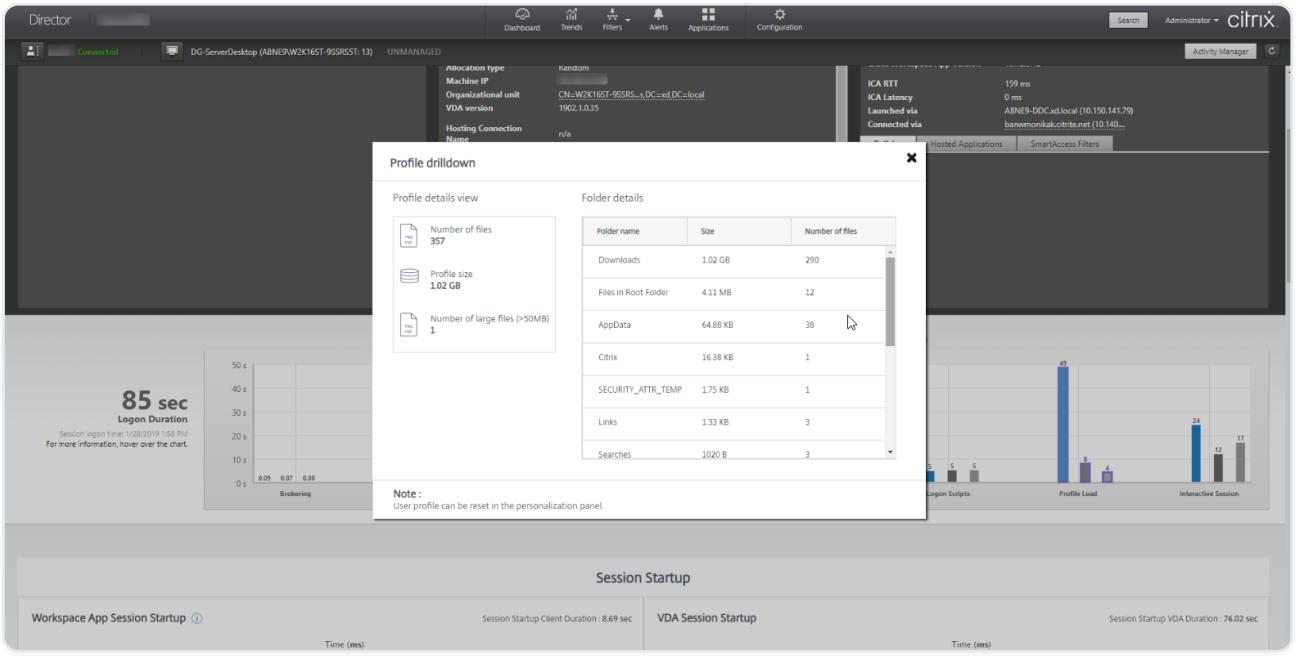
Se o Citrix Profile Management estiver configurado, a barra Carga de Perfil incluirá o tempo gasto pelo Citrix Profile Management para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management está configurado, a barra Carga de Perfil exibe uma duração aumentada.

Esse aumento é causado por essa melhoria e não reflete uma degradação de desempenho. Essa melhoria está disponível em VDAs 1903 ou posteriores.

Passar o mouse sobre a barra Carga de Perfil exibe uma dica de ferramenta mostrando os detalhes do perfil do usuário para a sessão atual.



Clique em **Detalhamento Detalhado** para detalhar ainda mais 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 na análise detalhada. Para ocultar a visibilidade da pasta, edite o seguinte valor de 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 são incluídos no detalhamento do perfil e exibidos na lista de arquivos em **Root Folder**.
- 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 de Personalização devido a certas limitações do Windows.

SESSÃO INTERATIVA

Este é o tempo levado 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 levado para cada subfase
- atraso de tempo cumulativo total entre essas subfases
- link para a documentação.

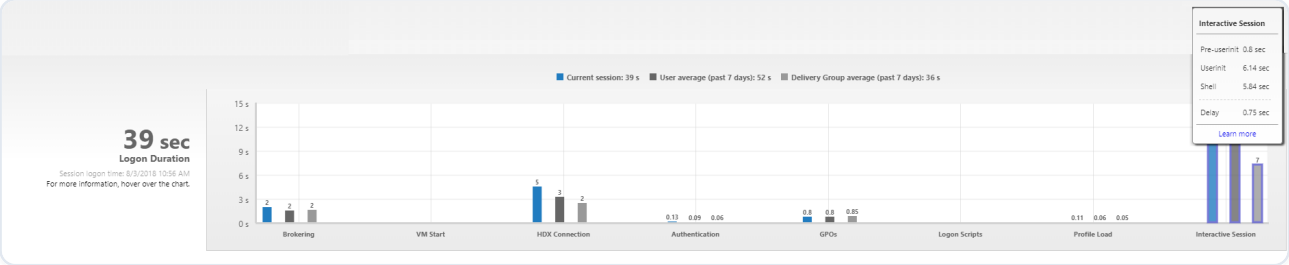
Nota:

Este recurso está disponível em VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores à versão 7.18 e depois atualizou para 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 processo 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, mais processamento ocorre, o que pode resultar em uma duração de logon mais longa do que a soma. O tempo total de logon não inclui o tempo ocioso do ICA®, que é o tempo entre o download do arquivo ICA e o lançamento do arquivo ICA para um aplicativo. Para habilitar a abertura automática do arquivo ICA no lançamento do aplicativo, configure seu navegador para o lançamento automático do arquivo ICA no 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 estiver lenta, o problema pode estar no hipervisor, então você pode escalá-lo para o administrador do hipervisor. Ou, se o tempo de corretagem estiver lento, você pode escalar o problema para o administrador do site para verificar o balanceamento de carga no Delivery Controller.

Examine as diferenças incomuns, incluindo:

- Barras de logon (atuais) ausentes
- Grande discrepância entre a duração atual e a duração média deste usuário. As causas incluem:
  - Uma nova aplicação foi instalada.
  - Uma atualização do sistema operacional ocorreu.
  - Alterações de configuração foram feitas.
  - O tamanho do perfil do usuário é alto. Neste caso, a Carga do Perfil é alta.
- Grande discrepância entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

Se necessário, clique em **Reiniciar** para observar o processo de logon do usuário para solucionar problemas, como Início da VM ou Corretagem.

Espelhar usuários

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 VDA do Windows são espelhadas usando o Assistência Remota do Windows. Habilite o recurso **Assistência Remota do Usuário do Windows** 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.

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

AÇÃO	DESCRIÇÃO
	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 logon novamente para que você possa verificar o aplicativo. 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 logon novamente.
Colocar a máquina em modo de manutenção	Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina em modo de manutenção. Na exibição Detalhes da Máquina, clique em Detalhes e ative a opção de modo de manutenção. Encaminhe para o administrador apropriado.

Restaurar conexões de desktop

No Director, verifique o status da conexão do usuário para a máquina atual na barra de título do usuário.

Se a conexão da área de trabalho falhou, o erro que causou a falha é exibido e pode ajudá-lo a decidir como solucionar o problema.

AÇÃO	DESCRIÇÃO
Certifique-se de que a máquina não esteja no modo de manutenção	Na página Detalhes do Usuário, certifique-se de que o modo de manutenção esteja desativado.

AÇÃO	DESCRIÇÃO
Reiniciar a máquina do usuário	Selecione a máquina e clique em **Reiniciar**. Use esta opção se a máquina do usuário não estiver respondendo ou não conseguir se conectar. Por exemplo, quando a máquina está usando uma quantidade incomumente alta de recursos da CPU, o que pode tornar a CPU inutilizável.

Restaurar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

Na exibição Detalhes do Usuário, solucione falhas de sessão no painel **Detalhes da Sessão**. Você pode visualizar os detalhes da sessão atual, indicados pelo ID da sessão.

AÇÃO	DESCRIÇÃO
Encerrar aplicativos ou processos que não estão respondendo	Clique na guia **Aplicativos**. Selecione qualquer aplicativo que não esteja respondendo e clique em **Encerrar Aplicativo**. Da mesma forma, selecione qualquer processo correspondente que não esteja respondendo e clique em **Encerrar Processo**. Além disso, encerre processos que estão consumindo uma quantidade incomumente alta de memória ou recursos da CPU, o que pode tornar a CPU inutilizável.
Desconectar a sessão do Windows	Clique em **Controle de Sessão** e selecione **Desconectar**. Esta opção está disponível apenas para máquinas de SO de múltiplas sessões intermediadas. Para sessões não intermediadas, a opção está 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 exibição **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 aparece, solicitando um local na máquina do Director para baixar o arquivo.

Redefinir um perfil de usuário

> **CUIDADO:**

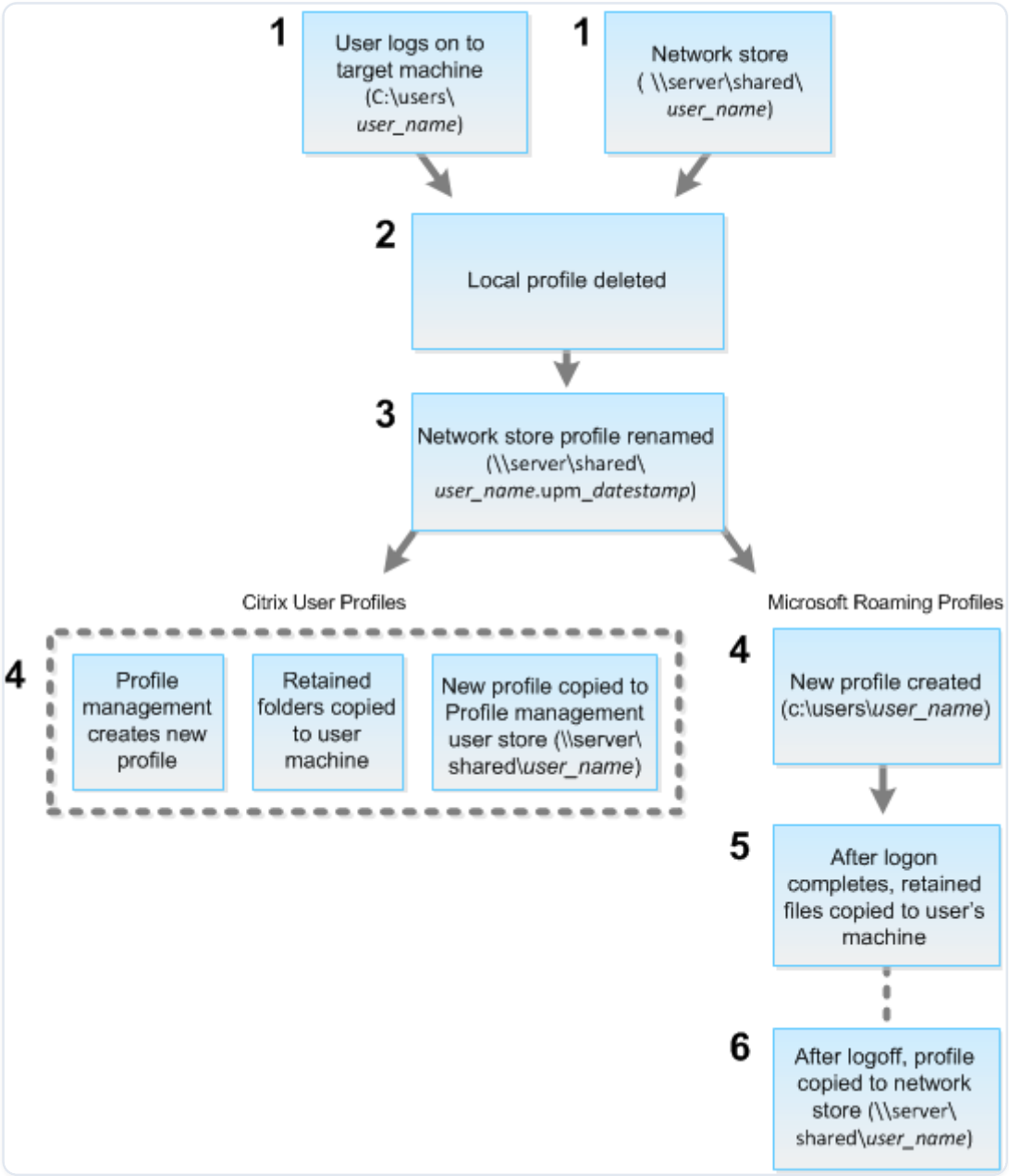
> Quando um perfil é redefinido, as pastas e arquivos do usuário são salvos e copiados para o novo perfil. No entanto, a maioria dos dados do perfil do usuário está ausente (por exemplo, o registro é redefinido e as configurações do aplicativo podem ser excluídas).

> A partir do Profile Management 2106, a função de redefinição está disponível para a solução de perfil de usuário baseada em contêiner de perfil do Citrix Management.

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 PowerShell SDK), o Director primeiro identifica o perfil de usuário em uso e emite um comando de redefinição apropriado. O Director recebe as informações através do Profile Management, incluindo informações sobre o tamanho, tipo e tempos de logon do perfil.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.



O comando de redefinição emitido pelo Director especifica o tipo de perfil. O serviço Profile Management então tenta redefinir um perfil desse tipo e procura o compartilhamento de rede apropriado (armazenamento de usuário). Se o usuário for processado pelo Profile Management, mas receber um comando de perfil móvel, ele será rejeitado (ou o contrário).

1. Se um perfil local estiver presente, ele será excluído.
2. O perfil de rede é renomeado.
3. A próxima ação depende se o perfil que está sendo redefinido é um perfil de usuário Citrix ou um perfil móvel da Microsoft.

   Para perfis de usuário Citrix, o novo perfil é criado usando as regras de importação do Profile Management. As pastas são copiadas de volta para o perfil de rede, e o usuário pode fazer logon normalmente. Se um perfil móvel for usado para a redefinição, quaisquer configurações de registro no perfil móvel serão preservadas no perfil redefinido. Você pode configurar o Profile Management para que um perfil de modelo substitua o perfil móvel, se necessário.

   Para perfis móveis da Microsoft, o Windows cria um perfil e, quando o usuário faz logon, as pastas são copiadas de volta para o dispositivo do usuário. Quando o usuário faz logoff novamente, o novo perfil é copiado para o armazenamento de rede.

Para redefinir um perfil de usuário no Director

Se você estiver usando o Citrix Virtual Desktops™ (Desktop VDA), faça o seguinte:

1. No **Director**, procure o usuário cujo perfil você deseja redefinir e, em seguida, selecione a sessão desse usuário.
2. Clique em **Redefinir Perfil**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente. As pastas e arquivos que foram salvos do perfil do usuário são copiados para o novo perfil.

Se você estiver usando o Citrix Virtual Desktops (Server VDA), 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 a fazer logon novamente primeiro no mesmo desktop ou aplicativo que ele relatou como

problema. Essa ação de logon garante que o perfil correto seja redefinido. Se o perfil for um perfil de usuário Citrix, ele já estará redefinido quando a área de trabalho do usuário aparecer. Se o perfil for um perfil móvel da Microsoft, a restauração da pasta ainda poderá estar em andamento por um breve período. O usuário deve permanecer logado até que a restauração seja concluída.

Se o perfil não for redefinido com 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 de perfil de usuário completa, 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 específico. 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 gera uma pasta de backup nomeada pela data e hora atuais.

Redefinir um perfil de roaming do Windows

- Suponha que você queira redefinir o perfil de roaming para user1. Use o comando PowerShell New-BrokerMachineCommand. Por exemplo:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

Gravar sessões

Você pode gravar sessões ICA® usando os controles de Gravação de Sessão nas telas de **Detalhes do Usuário** e **Detalhes da Máquina** no Director. Este recurso está disponível para clientes em sites **Premium**.

Para configurar a Gravação de Sessão no Director usando a ferramenta DirectorConfig, consulte a seção **Configurar o Director para usar o Servidor de Gravação de Sessão** em Criar e ativar políticas de gravação. Os controles de Gravação de Sessão estão disponíveis no Director somente se o usuário logado tiver permissão para modificar as políticas de Gravação de Sessão. Essa permissão pode ser definida no console de Autorização de Gravação de Sessão, conforme descrito em Criar e ativar políticas de gravação.

> **Nota:** As alterações feitas nas configurações de Gravação de Sessão através do Director ou do console da Política de Gravação de Sessão entram em vigor a partir da sessão ICA subsequente.

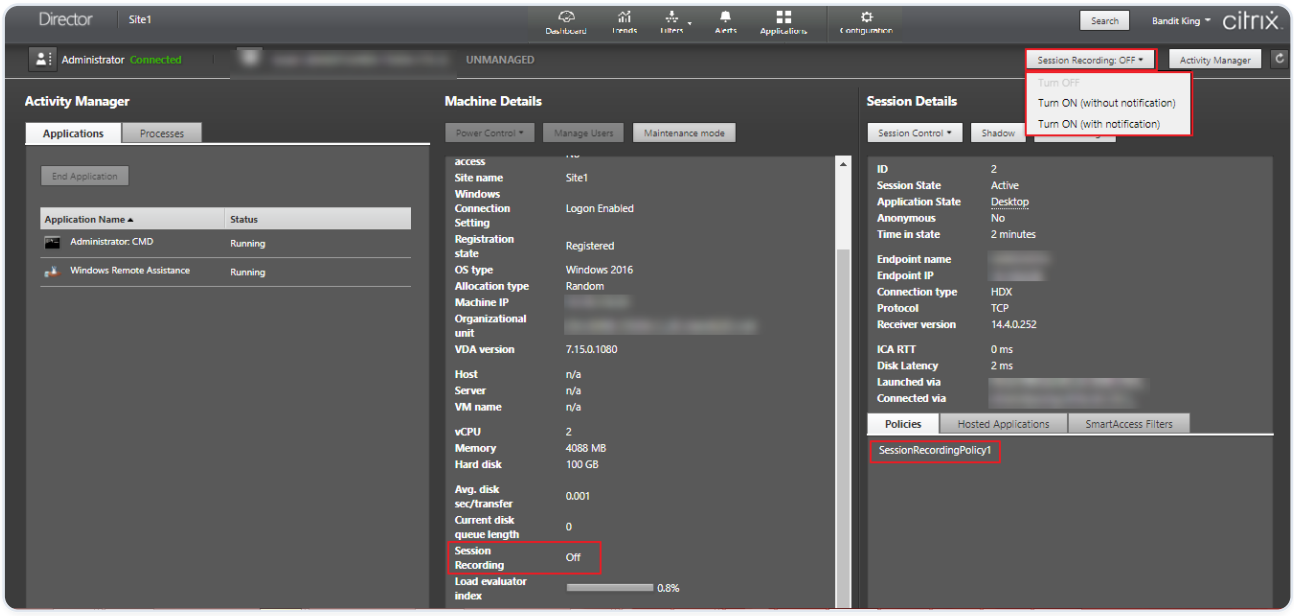
Controles de Gravação de Sessão no Director

Você pode habilitar a Gravação de Sessão para um usuário específico na tela **Gerenciador de Atividades** ou **Detalhes do Usuário**. As sessões subsequentes são gravadas para o usuário específico em todos os servidores suportados.

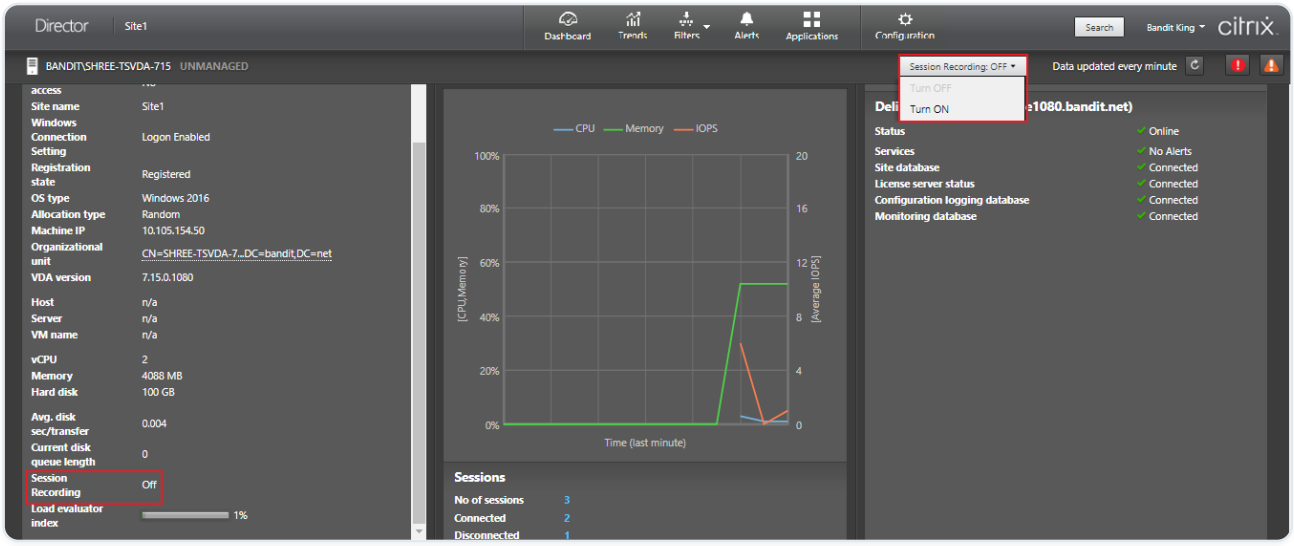
Você pode:

- Ativar (com notificação) - o usuário é notificado sobre a sessão sendo gravada ao fazer logon na sessão ICA.
- Ativar (sem notificação) - a sessão é gravada silenciosamente sem notificar o usuário.
- Desativar - desabilitar a gravação de sessões para o usuário.

O painel **Políticas** exibe o nome da política de Gravação de Sessão ativa.



Você pode habilitar a Gravação de Sessão para uma máquina específica na página Detalhes da Máquina. As sessões subsequentes na máquina são gravadas. O painel **Detalhes da Máquina** exibe o status da política de Gravação de Sessão para a máquina.



Matriz de compatibilidade de recursos

O Citrix Director 7 2203 é compatível com:

- Citrix Virtual Apps and Desktops™ 7 2112 e posterior
- Citrix Virtual Apps 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 será realizada nos sites configurados. Se algum site estiver executando uma versão do Controller anterior à do Director, uma mensagem aparecerá no console do Director, recomendando uma atualização do site. Além disso, enquanto a versão do site for mais antiga que a do Director, uma nota permanecerá exibida no Painel do Director indicando essa incompatibilidade.

Observação:

Versões anteriores do Citrix Director não exibem políticas aplicadas a sessões de usuário executadas em versões recentes do VDA. O Citrix Director 1912 e versões anteriores não exibem políticas aplicadas a sessões de usuário executadas em versões do VDA 2003 e posteriores. Use as versões 2003 e posteriores do Citrix Director para visualizar essas políticas.

Recursos específicos do Director com a versão mínima do Delivery Controller (DC), VDA e outros componentes dependentes necessários, juntamente com a Edição da Licença, estão listados abaixo.

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
1909	Configurar sites locais com o Citrix Analytics for Performance	DC 7 1906 e VDA 1906	Todas

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
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 do Microsoft RDS	DC 7 1811 e VDA 7.16	Todos
1808	Exportação de dados de filtros	DC 7 1808	Todos
1808	Detalhamento da sessão interativa	DC 7 1808 e VDA 1808	Todos
1808	Detalhamento de GPO	DC 7 1808 e VDA 1808	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
1808	Dados históricos da máquina disponíveis usando a API OData	DC 7 1808	Todos
7.18	Sondagem de aplicativo	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 Shadow Linux VDA	VDA 7.16	Todos
7.16	Suporte a grupos locais de domínio	Nenhum	Todos
7.16	Acesso ao console da máquina	DC 7.16	Todos
7.15	Monitoramento de falhas de aplicativos	DC 7.15 e VDA 7.15	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
7.14	Solução de problemas centrada em aplicativos	DC 7.13 e VDA 7.13	Todos
7.14	Monitoramento de Disco	DC 7.14 e VDA 7.14	Todos
7.14	Monitoramento de GPU	DC 7.14 e VDA 7.14	Todos
7.13	Protocolo de transporte no painel Detalhes da Sessão	DC 7.x e VDA 7.13	Todos
7.12	Descrições de falha de conexão e máquina fáceis de usar	DC 7.12 e VDA 7.x	Todos
7.12	Disponibilidade de dados históricos aumentada na edição Enterprise	DC 7.12 e VDA 7.x	Enterprise
7.12	Relatórios Personalizados	DC 7.12 e VDA 7.x	Premium (anteriormente Platinum)
7.11	Relatórios de utilização de recursos	DC 7.11 e VDA 7.11	Todos
7.11	Alertas estendidos para condições de CPU, memória e RTT ICA	DC 7.11 e VDA 7.11	Premium (anteriormente Platinum)

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
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 alerta proativos	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)
7.7	Integração SCOM	DC 7.7, VDA 7.x, SCOM 2012 R2 e PowerShell 3.0	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 com 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 da sessão do usuário, detalhes de desempenho de logon do usuário, detalhes de balanceamento de carga da sessão e informações de falha de conexão e máquina. Os dados são agregados de forma diferente dependendo de sua categoria. Compreender a agregação de valores de dados apresentados usando as APIs de 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 agregado. 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 (Interval=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, extraindo 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 o fim do período de tempo.
- **Eventos perdidos e latentes.** As métricas agregadas na tabela de resumo podem ser ligeiramente imprecisas se os eventos forem perdidos ou latentes para o período de agregação. Embora o Serviço de Monitoramento tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo para eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a 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 inferior (minutos) são limpos mais rapidamente do que dados de granularidade superior (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles poderão ser encontrados em uma granularidade superior. Como as chamadas de API retornam apenas a granularidade específica solicitada, não receber dados para uma granularidade não significa que os dados não existam para uma granularidade superior para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de data/hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não se

enquadram nos limites por hora, pode haver alguma discrepância quanto ao local onde os dados são agregados.

Granularidade e retenção

A granularidade dos dados agregados recuperados pelo 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. Em caso de 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 de Logon por Sessão de 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 "Load Evaluator Index" 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 Hipervisor 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	Esta configuração afeta os Alertas exibidos no Monitor.	90	Não aplicável
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	Esta configuração afeta os gráficos de CPU e Memória vistos na página de Detalhes da Máquina em "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	Esta configuração afeta os gráficos de CPU e Memória para o Período de Tempo "Últimas 2 Horas" vistos na página de Detalhes da Máquina em “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 "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 orientação 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, já que 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 somente em sites com licença Premium.
- GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays são limitados a 31 dias em sites com licença Premium.

Reter dados por longos períodos tem as seguintes implicações nos tamanhos das tabelas:

- **Dados por hora.** Se os dados por hora puderem permanecer no banco de dados por até dois anos, um site 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 no servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto dramático no desempenho.
- **Dados de sessão e evento.** Dados coletados toda vez que uma sessão é iniciada e uma conexão/reconexão é feita. Para um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, dois anos de dados dessas tabelas acumulariam mais de um TB de dados, exigindo um banco de dados de nível empresarial de ponta.

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] MachineFailure	[2] SessionPreparation	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] MachineFailure	[3] RegistrationTimeout	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 delivery controller e se o Desktop service está em execução no VDA. Inicie cada um se estiverem parados.
[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] NenhumaLicençaDisponível	[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 defeito. 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 do VDA depois que o cliente	Verifique se a sessão não foi encerrada pelo usuário antes do

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		contatou inicialmente o VDA, mas antes de concluir a sequência de conexão.	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 broker ainda estava inicializando, ou um erro interno durante a fase de intermediação de um lançamento.	Verifique se o Serviço de Broker da Citrix está em execução e tente iniciar a sessão novamente.
[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 desabilitado pelo administrador.	Se o aplicativo for destinado a estar disponível para uso em produção, habilite o aplicativo e instrua o usuário a reconectar.

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[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 cobertos pela edição e tipo de licença existentes do Citrix Virtual Apps and Desktops™.
[3] Nenhuma Capacidade Disponível	[13] Limite de Sessões Atingido	Todos os VDAs estão em uso e não há capacidade para hospedar mais sessões. Causas possíveis: Todos os VDAs estão em uso (para VDAs de SO de sessão única), ou todos os VDAs atingiram o número máximo configurado de sessões simultâneas permitidas (para VDAs de SO de múltiplas sessões).	Verifique se há VDAs em modo de manutenção. Desative o modo de manutenção se não for necessário para liberar mais capacidade. Considere aumentar o valor de **Número Máximo de Sessões** na configuração da política Citrix para permitir mais sessões por VDA de servidor. Considere adicionar mais VDAs de SO de múltiplas sessões. Considere adicionar mais VDAs de SO de sessão única.
[5] Configuração	[14] Protocolo Não Permitido	Os protocolos ICA e RDP não são permitidos.	Execute o comando PowerShell **Get-BrokerAccessPolicyRule** no delivery controller e verifique se o valor de

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
			AllowedProtocols lista todos os protocolos desejados. Este problema ocorre apenas se houver uma configuração incorreta.
[5] Configuração	[15] Recurso Indisponível	O aplicativo ou desktop ao qual o usuário está tentando se conectar não está disponível. Este aplicativo ou desktop pode não existir, ou não há VDAs disponíveis para executá-lo. Causas possíveis: O aplicativo ou desktop foi despublicado, ou os VDAs que hospedam o aplicativo ou desktop atingiram a carga máxima, ou o aplicativo ou desktop está definido em modo de manutenção.	Verifique se o aplicativo ou desktop ainda está publicado e se os VDAs não estão em modo de manutenção. Determine se os VDAs de SO de múltiplas sessões estão com carga total. Se sim, provisione mais VDAs de SO de múltiplas sessões. Verifique se há VDAs de SO de sessão única disponíveis para conexões. Provisione mais VDAs de SO de sessão única, se necessário.
[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	No controlador de entrega, verifique se a **Reconexão de Sessão Ativa** está habilitada. Verifique se o valor de **DisableActiveSessionReconnect** no registro, em

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		se conectar à sessão ativa.	**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 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	Verifique via ping, se o controlador de entrega e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		ativamente essa solicitação.	de firewall ou roteamento de rede.
[2] MachineFailure	[20] Falha de ConfigurationSet	O controlador de entrega 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 controlador e o VDA, problemas encontrados pelo Serviço de Broker ao criar uma solicitação de conjunto de configuração, ou problemas de rede que resultam no VDA não aceitando a solicitação.	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	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.

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	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] ClientConnectionFailure	[23] Erro de comunicação	O controlador de entrega tentou enviar informações para o VDA, como uma solicitação para preparar uma conexão, mas ocorreu um erro durante a tentativa de comunicação. Isso pode ser causado por interrupções de rede.	Se já iniciado, reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verificar se o VDA se registra com sucesso. Confirme se os controladores de entrega configurados para o VDA estão corretos por meio dos detalhes no log de eventos do aplicativo.
[3] NoCapacityAvailable	[100] NoMachineAvailable O serviço de monitoramento converte [12] NoDesktopAvailable	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	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se há VDAs suficientes

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
	para este código de erro.	indisponível, o VDA não foi reiniciado 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.	registrados e em estado pronto para poder iniciar o desktop compartilhado publicado ou o aplicativo solicitado pelo usuário. Verifique se o hipervisor que hospeda o VDA não está em modo de manutenção.
[2] MachineFailure	[101] MachineNotFunctional. O serviço de monitoramento converte [12] NoDesktopAvailable para este código de erro.	O VDA não está operacional. Causas possíveis: O VDA foi removido do grupo de entrega, o VDA está não registrado, o estado de energia do VDA está indisponível, ou o VDA está enfrentando problemas internos.	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se o VDA aparece como ligado no Citrix Studio. Se o estado de energia for desconhecido para várias máquinas, resolva quaisquer problemas de conectividade com o hipervisor ou falhas 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	-	-
Capacidade Máxima (representada como Carga Máxima no Console do 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.
PresoNaInicialização	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 do SO. Certifique-se de que as ferramentas do hipervisor estejam instaladas na VM. Certifique-se de que o VDA esteja instalado na VM.
FalhaAoIniciar	1	A VM apresentou 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
DesligamentoDoAgente	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.
AgenteSuspenso	1	O VDA está em hibernação ou modo de suspensão.	Tire o VDA do modo de hibernação. Considere desabilitar a hibernação para VDAs do Citrix Virtual Apps and Desktops através das configurações de energia.
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

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			contrário, corrija-os. Se for generalizado, valide as configurações de DNS nos delivery controllers. Verifique a resolução de DNS 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.
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

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			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 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 controlador do site	Certifique-se de que a configuração do Active Directory esteja correta ou verifique as configurações do registro.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		são armazenadas no AD) configurada no registro do VDA é para um Site diferente.	
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.
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	Alinhe as versões do VDA e do delivery controller.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		solicitação de registro.	
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 Credencial de Segurança Não Suportada	109	O VDA e o delivery controller não estão usando o mesmo mecanismo de criptografia.	Alinhe as versões do VDA e do delivery controller.
InvalidRegistrationRequest	110	O VDA fez uma solicitação de registro 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 delivery controllers no Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controller e o VDA.
SingleMultiSessionMismatch	111	O tipo de sistema operacional do VDA não é compatível com o catálogo de	Adicione o VDA ao tipo de catálogo de máquinas ou grupo de entrega correto

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		máquinas ou grupo de entrega.	que contenha máquinas com o mesmo sistema operacional.
FunctionalLevelTooLowForCatalog	112	O catálogo de máquinas está definido 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 downgrade do catálogo de máquinas para corresponder ao do VDA.
FunctionalLevelTooLowForDesktopGroup	113	O grupo de entrega está definido 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 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

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			VDA assim que ele estiver novamente ativo 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 atualizações forem incompatíveis com a versão do VDA instalada.	Atualize o VDA se necessário. Verifique se as atualizações aplicadas são compatíveis com a versão do VDA.
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 na 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

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			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 através dos detalhes no log de 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 controlador de entrega perdeu a conexão com o VDA. Isso pode ser causado por interrupções de rede.	Verifique se o serviço Desktop está em execução no VDA. Inicie-o se estiver parado.
BrokerRegistrationLimitReached	301	O controlador de entrega atingiu o número máximo configurado de VDAs que podem se registrar simultaneamente. Por padrão, o	Considere adicionar controladores de entrega ao Site ou criar um Site. Você também pode aumentar o número de VDAs permitidos para se registrar

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		controlador de entrega permite 10.000 registros simultâneos de VDA.	simultaneamente com o controlador de entrega por meio da chave de registro **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers**. Consulte o artigo da Central de Conhecimento, Entradas de Chave de Registro Usadas pelo Citrix Virtual Apps and Desktops (CTX117446) para obter mais informações. Aumentar esse número pode exigir mais recursos de CPU e memória para o controlador.
SettingsCreationFailure	208	O Broker não construiu um conjunto de configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falhará e o VDA ficará não registrado.	Verifique os logs de eventos no controlador de entrega para quaisquer erros. Reinicie o Serviço Broker se um problema específico não for evidente nos logs. Uma vez que o Serviço Broker seja reiniciado, reinicie o serviço Desktop nos VDAs afetados e verifique se eles se

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			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 dados de configuração para o VDA. Se o Broker puder coletar os dados, mas não conseguir enviá-los, o registro falhará.	Se limitado a um único VDA, reinicie o serviço Desktop no VDA para forçar o novo registro e valide se o VDA se registra com sucesso através do log de eventos do aplicativo. Solucione quaisquer erros observados. Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			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.
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.

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 da Política de Grupo do Citrix podem ser instalados como um módulo ou um snap-in. Vários SDKs de componentes (como Citrix Licensing, Citrix Provisioning e StoreFront) são instalados usando apenas um snap-in.

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

SDK do Citrix Virtual Apps and Desktops

Este SDK é instalado automaticamente como um módulo 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 do Citrix. Embora os membros do grupo de administradores locais no Controller tenham automaticamente privilégios administrativos completos para permitir que o Citrix Virtual Apps ou o Citrix Virtual Desktops™ sejam instalados, o Citrix recomenda que, para operação normal, você crie administradores Citrix com os direitos apropriados, em vez de usar a conta de administradores locais.

Acessar e executar os cmdlets

1. Inicie um shell no PowerShell: Abra o Studio, selecione a guia **PowerShell** e clique em **Launch PowerShell**.

2. Para usar cmdlets do SDK em scripts, defina a política de execução no PowerShell. Para obter informações sobre a política de execução do PowerShell, consulte a documentação da Microsoft.
3. Se você quiser usar o snap-in (em vez do módulo), adicione o snap-in usando o cmdlet `Add-PSSnapin` (ou `asnp`).

   V1 e V2 denotam a versão do snap-in. Os snap-ins do XenDesktop 5 são a versão 1. Os snap-ins do Citrix Virtual Apps and Desktops e das versões anteriores do XenDesktop 7 são a versão 2. Por exemplo, para instalar o snap-in do Citrix Virtual Apps and Desktops, digite `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Para importar todos os cmdlets, digite: `Add-PSSnapin Citrix.*.Admin.V*`

Agora você pode usar os cmdlets e os arquivos de ajuda.

- Para acessar os arquivos de ajuda para este SDK, selecione o produto ou componente na lista Categorias e, em seguida, selecione **Citrix Virtual Apps and Desktops SDK**.
- Para obter orientação sobre PowerShell, consulte Windows PowerShell Integrated Scripting Environment (ISE).

SDK da Política de Grupo

O SDK da Política de Grupo do Citrix permite exibir e configurar as configurações e filtros da Política de Grupo. Este SDK usa um provedor PowerShell para criar uma unidade virtual que corresponde às configurações e filtros de máquina e usuário. O provedor aparece como uma extensão para `New-PSDrive`.

Para usar o SDK da Política de Grupo, o Studio ou o SDK do Citrix Virtual Apps and Desktops deve estar instalado.

O provedor PowerShell de Política de Grupo do 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

Controlador é o nome de domínio totalmente qualificado de um Controlador no site ao qual você deseja se conectar e carregar as configurações.

OData do Serviço de Monitoramento

A API do Monitor permite o acesso aos dados do Serviço de Monitoramento usando a Versão 3 ou 4 da API OData. Você pode criar painéis de monitoramento e relatórios personalizados com base nos dados consultados do Serviço de Monitoramento. O OData V.4 é baseado na API Web ASP.NET e oferece suporte a consultas de agregação.

Para obter mais informações, consulte a API OData do Serviço de Monitoramento.

__index__

Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site.

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar 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 com licença não Premium e não 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 de tempo é definido como Último mês (**Terminando agora**) ou menor. Para o período de tempo escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendências estão disponíveis como gráficos e não como tabelas.
- Os valores de retenção de limpeza do Monitor Service 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

Ver tendências para sessões: Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas de Confiabilidade da Sessão ou 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 perfeita. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período selecionado nos Filtros. Um detalhamento fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Este recurso requer o Delivery Controller™ versão 7 1906 ou posterior, e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações 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 Controladores de Entrega descartam as cargas úteis 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 visualização 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 de 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 que é 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 somente 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 visualização 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 visualização 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.

> **Nota:**
>
> Muitos processos listados nesta tabela podem consumir uma grande quantidade de dados, afetando o desempenho. Para evitar isso, são listados apenas os processos com CPU Média ou Memória Média superior a 1%. Assim, a tabela pode, às vezes, listar menos de 10 processos.

Filtre por Grupo de Entrega e Período. Os gráficos de CPU, uso de 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 Top 10 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).

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 visualização contextual de usuário, aplicativo e desktop da rede. 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

Visualizar falhas de aplicativo: A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. São suportados VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de múltiplas sessões executando Windows Server 2008 e posterior. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas as falhas de aplicativo de VDAs de SO de múltiplas sessões são exibidas. Você pode definir o monitoramento de falhas de aplicativo usando políticas de monitoramento. Para obter mais informações, consulte Configurações da política de monitoramento.

Visualizar resultados da sondagem de aplicativos: A guia Resultados da Sondagem de Aplicativos exibe os resultados da sondagem para aplicativos que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha de inicialização do aplicativo ocorreu é registrado.

Este recurso requer Delivery Controller(s) e VDAs **versão 7.18** ou posterior. Para obter mais informações, consulte Sondagem de aplicativos.

Criar relatórios personalizados: A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados em tempo real e históricos do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatórios Personalizados salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente, ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique as 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 na Visualização e no relatório de 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 da conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
- Os Grupos de Entrega excluídos no 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.